UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

DESARROLLO DE UNA APLICACIÓN DE SOFTWARE PARA LA VALIDACIÓN DE LOS FORMATOS OFICIALES DE FIRMA DIGITAL DENTRO DEL SISTEMA NACIONAL DE CERTIFICACIÓN DIGITAL DE COSTA RICA

Trabajo final de investigación aplicada sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Computación e Informática para optar al grado y título de Maestría Profesional en Computación e Informática

José Luis Villegas Castillo

Ciudad Universitaria Rodrigo Facio, Costa Rica
2019

A Dios,
por brindarme la vida, por ser mi guía en todo momento
y por darme las fuerzas necesarias para seguir adelante.

A mi esposa, mis padres y mis hermanas,
por su amor y apoyo incondicional,
por impulsarme siempre a crecer y a ser una mejor persona.

--JL

Agradecimientos

Quiero agradecer de forma muy especial al Dr. Ricardo Villalón Fonseca, por su dedicación, apoyo y paciencia durante el desarrollo de este proyecto. Su guía y motivación fueron muy importantes para poder concluirlo satisfactoriamente.

También, quiero dar las gracias a la Dra. Gabriela Marín Raventós por su comprensión y apoyo durante los últimos meses.

Finalmente, muchas gracias a los profesores de la Maestría Profesional en Computación de la Universidad de Costa Rica, por su dedicación y enseñanzas durante los años que estuve cursando la maestría.

Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Computación e Informática de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Computación e Informática.

Dra. Gabriela Barrantes Sliesarieva
Representante del Decano
Sistema de Estudios de Posgrado

Dr. Ricardo Villalón Fonseca
Profesor Guía

Dra. Gabriela Marín Raventós
Directora del Programa
de Posgrado en Computación e Informática

José Luis Villegas Castillo
Sustentante

Índice

Resumen

En el año 2014 el Gobierno de Costa Rica emitió la directriz 067-MICITT-H-MEIC, la cual faculta a los ciudadanos a exigir que las instituciones del estado brinden sus servicios electrónicamente utilizando firma digital.

La publicación de esta directriz conlleva un esfuerzo enorme de parte de las entidades que soportan la implementación de firma digital en el país, para proveerle a los usuarios, guías y herramientas de ejemplo que les ayude en el uso e implementación de firma digital. Sin embargo, a pesar de estos esfuerzos no tienen herramientas disponibles para la firma y validación de todos los formatos oficiales de firma de documentos.

El objetivo principal de este proyecto de investigación fue desarrollar una aplicación de software para la validación de los formatos oficiales dentro del Sistema Nacional de Certificación Digital (SNCD), que pueda ser tomada en cuenta para formar parte de las herramientas de ejemplo de firma y validación de documentos firmados digitalmente. Primero, se realizó una revisión sistemática de los documentos oficiales sobre firma digital del Gobierno de Costa Rica para identificar los perfiles oficiales de los formatos de firma digital. Luego, se seleccionó un perfil para validarlo con la aplicación. Posteriormente, se procedió al desarrollo de la aplicación con base en los requerimientos técnicos de los estándares de la ETSI y en la migración de una librería desarrollada por la Unión Europea que valida las firmas de acuerdo con estos estándares. Finalmente, se validó la aplicación desde el punto de vista funcional y de seguridad. Para la validación de seguridad se realizó un análisis estático de código y se evaluó la aplicación con la "*Guía de requerimientos técnicos para el aseguramiento de la información de los componentes tecnológicos que utilizan certificados y firma digital en aplicaciones de software dentro del Sistema Nacional de Certificación Digital"*, elaborada por Alejandro Mora.

Como resultado se desarrolló una aplicación fiable y segura para la validación de documentos firmados digitalmente dentro del SNCD. Esta investigación se enmarca en el proyecto "Desarrollo de esquemas para certificar autoridades certificadoras y aplicaciones de software en el SNCD" del Centro de Investigaciones en Tecnologías de la Información y la Comunicación de la Universidad de Costa Rica.

Abstract

In the year 2014, the Government of Costa Rica issued the directive 067-MICITT-H-MEIC which empowers citizens to demand that state institutions provide their services electronically using digital signature.

The publication of this directive involves a huge effort from the entities that support the implementation of digital signature in the country, to provide guides and tools to the users, to help them in the use and implementation of digital signatures. However, despite these efforts they do not have available tools for signing and validating all official document signing formats.

The main objective of this research project was to develop a software application for the validation of the official document signing formats within the Sistema Nacional de Certificación Digital (SNCD), which can be considered to be part of the example tools for signature and validation of digitally signed documents. First, a systematic review of the official documents on the digital signature of the Government of Costa Rica was carried out to identify the official profiles of the digital signature formats. Then, a profile was selected to validate it with the application. Subsequently, the application was developed based on the technical requirements of the ETSI standards and the migration of a library developed by the European Union that validates the signatures in accordance with these standards. Finally, the application was validated from the functional and security point of view. For the security validation a static code analysis was performed and the application was evaluated with the guide "*Guía de requerimientos técnicos para el aseguramiento de la información de los componentes tecnológicos que utilizan certificados y firma digital en aplicaciones de software dentro del Sistema Nacional de Certificación Digital*", developed by Alejandro Mora.

As a result, a reliable and secure application for the validation of digitally signed documents within the SNCD was developed. This research is part of the project "Desarrollo de esquemas para certificar autoridades certificadoras y aplicaciones de software en el SNCD" of the Centro de Investigaciones en Tecnologías de la Información y la Comunicación of the Universidad de Costa Rica.

Índice de Tablas

Índice de Figuras

Índice de Abreviaturas

BCCR	Banco Central de Costa Rica
BES	*Basic Electronic Signature*
CA	Autoridad Certificadora
CAdES	*CMS Advanced Electronic Signatures*
CAMTIC	Cámara de Tecnologías de Información y Comunicación
CEF Digital	*Connecting Europe Facility Digital*
CMS	*Cryptographic Message Syntax*
CONARE	Consejo Nacional de Rectores
CRL	*Certificate Revocation List*
DCFD	Dirección de Certificadores de Firma Digital
DES	*Data Encryption Standard*
DSS	*Digital Signature Service*
EPES	*Explicit Policy Electronic Signature*
ESI	*Electronic Signatures and Infrastructures*
ETSI	*European Telecommunications Standards Institute*
ETSI EN	*ETSI European Standard, telecommunications series*
ETSI TS	*ETSI Technical Specification*
EU	*European Union*
ID	Identificador
IIS	*Internet Information Services*
ISO	*International Organization for Standardization*
LTV	*Long Term Validation*
MEIC	Ministerio de Economía, Industria y Comercio
MICITT	Ministerio de Ciencia, Tecnología y Telecomunicaciones
NA	No Aplica
OCSP	*Online Certificate Status Protocol*
OWASP	*Open Web Application Security Project*
PAdES	*PDF Advanced Electronic Signature*
PDF	*Portable Document Format*

PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
RA	Autoridad de Registro
RFC	*Request for Comments*
RSA	Algoritmo Rivest-Shamir-Adleman
SINPE	Sistema Nacional de Pagos Electrónicos
SNCD	Sistema Nacional de Certificación Digital
TFIA	Trabajo Final de Investigación Aplicada
TLS	*Transport Layer Security*
TSA	Autoridad de Estampado de Tiempo
TSL	*Trusted Service List*
UCR	Universidad de Costa Rica
XAdES	*XML Advanced Electronic Signature*
XL	*eXtended Long*
XML	*Extensible Markup Language*

1. Introducción

En el 2014 el Gobierno de Costa Rica emitió la directriz 067-MICITT-H-MEIC [1], la cual faculta a los ciudadanos a exigir que las instituciones del estado brinden sus servicios electrónicamente utilizando firma digital. Con esta directriz las instituciones tienen el deber de permitir a los usuarios autenticarse en sus sistemas por medio de firma digital y deben poner a su disposición los diferentes trámites que brindan de forma física utilizando la firma digital de documentos y de transacciones electrónicas.

La publicación de esta directriz conlleva un esfuerzo enorme de las instituciones del estado para digitalizar sus servicios e implementar firma digital para autenticación y firma de documentos. De igual manera, ha requerido de grandes esfuerzos por parte de las entidades que soportan la implementación de firma digital en el país, para proveerle a estas instituciones, documentación y herramientas que les ayuden en la implementación. Específicamente, en el área de firma digital de documentos, han generado guías para firmar y validar correctamente documentos con base en los formatos oficiales que se establecen en la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente [2]. También, han desarrollado herramientas de ejemplo para la firma y validación de documentos. Sin embargo, a pesar de estos esfuerzos no tienen herramientas disponibles para todos los formatos oficiales.

Este Trabajo Final de Investigación Aplicada (TFIA) se desarrolla como parte de ese esfuerzo de desarrollar y proveer herramientas de ejemplo para la firma y validación de los formatos oficiales de firma digital. En él se desarrolla una aplicación para la validación de firma que eventualmente podría ser tomada en cuenta para formar parte de las herramientas de ejemplo. Esta investigación se enmarca en el proyecto “Desarrollo de esquemas para certificar autoridades certificadoras y aplicaciones de software en el Sistema Nacional de Certificación Digital” del Centro de Investigaciones en Tecnologías de la Información y la Comunicación de la Universidad de Costa Rica.

En las siguientes secciones de este capítulo se contextualiza la investigación y se explica la estructura del presente documento.

1.1. Antecedentes

En Costa Rica, la Ley 8454 *Ley de Certificados, Firmas Digitales y Documentos Electrónicos* (Gobierno de Costa Rica, 2005) [3], establece el marco legal del uso de certificados y firmas digitales. Esta ley fue aprobada en agosto del año 2005 y con ella se les brindó respaldo legal a las acciones llevadas a cabo por medio de transacciones y documentos electrónicos. También, inicia la posibilidad de vincular jurídicamente a los actores involucrados en transacciones electrónicas.

En abril del 2006 se publicó el *Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos* (Gobierno de Costa Rica, 2006) [4], el cual complementa la Ley. Este reglamento fue redactado por una comisión integrada por funcionarios del Ministerio de Ciencia y Tecnología (MICITT), el Banco Central de Costa Rica (BCCR), el Poder Judicial, Procuraduría Nacional de la República, el Registro Nacional, Cámara de Tecnologías de Información y Comunicación (CAMTIC) y CONARE.

En este reglamento se define con un mayor grado de detalle la manera de implementar la firma digital en Costa Rica y junto con la Ley regula los actores del Sistema Nacional de Certificación Digital (SNCD). También, establece la Dirección de Certificadores de Firma Digital (DCFD) como certificadora raíz y como un ente adscrito al MICITT encargado de proveer regulaciones, requisitos y políticas del sistema [4]. La DCFD a su vez ha oficializado diversas políticas que han complementado la forma de implementar la firma digital en el SNCD, por ejemplo, en el 2008 entran en vigencia la Política de certificados para la jerarquía nacional de certificadores registrados [5] y la Política de sellado de tiempo del Sistema Nacional de Certificación Digital [6], las cuales incluyen las obligaciones de las Autoridades Certificadoras (CA por sus siglas en inglés) y de las Autoridades de Sellado de Tiempo (TSA por sus siglas en inglés), respectivamente. De igual manera, en el 2013 se oficializa la Política

de formatos oficiales de los documentos electrónicos firmados digitalmente, en donde se establecen los formatos oficiales de documentos firmados electrónicamente y sus características [2].

Dado que la DCFD no contaba con la capacidad tecnológica para cumplir con los requerimientos de una certificadora raíz, cuando se publicó el reglamento a la ley (2006), el MICITT firma un convenio con el BCCR para que esta entidad implemente y custodie la raíz del sistema, y se convierta en el encargado de la implementación tecnológica de firma digital en el país. Desde el 2008 se logró poner en funcionamiento la CA raíz del SNCD y en el 2009 el BCCR creó la autoridad emisora certificadora SINPE para entregar certificados digitales. Desde entonces el BCCR se ha dado la tarea de proveer la infraestructura para que la certificación y firma digital funcione en el país, lo cual ha sido muy beneficioso gracias a sus avances tecnológicos en temas de seguridad.

En el 2014 el Gobierno emitió la directriz 067-MICITT-H-MEIC en el diario oficial La Gaceta, en la que decretó que todas las instituciones públicas deben brindar todos sus servicios de forma electrónica [1]:

> *Artículo 3°-Todo nuevo desarrollo, funcionalidad o implementación de sistemas de información de las instituciones del sector público costarricense, en los cuales se ofrezcan servicios de cara al ciudadano o de utilización interna, deberá incorporar:*
>
> *a. Mecanismos de autenticación mediante firma digital certificada. Cuando un ciudadano se autentique utilizando firma digital certificada, se reconocerá la autenticidad plena y el valor de su relación con la institución por el canal electrónico.*
>
> *b. Mecanismos de firma de documentos y transacciones electrónicas mediante firma digital certificada cuando el trámite así lo requiera, tanto para uso de los funcionarios como para los ciudadanos involucrados en el proceso.*

Dada esta directriz, en los últimos años ha aumentado la cantidad de instituciones que utilizan la firma digital para la autenticación de personas y para la firma de documentos. Sin embargo, aún existen retos técnicos a nivel país que deben superarse. Por ejemplo, se carece de una herramienta oficial que permita validar el formato de la firma de los documentos generados por dichas instituciones. En documentos de acceso público que ha desarrollado la DCFD se hacen recomendaciones de herramientas de terceros para firmar documentos válidos y acorde con los formatos establecidos, pero no se hace recomendación de una aplicación que facilite la validación de estos documentos. Una herramienta de este tipo es muy importante para que las instituciones puedan verificar que las aplicaciones, que han desarrollado o adquirido, están firmando documentos con formatos válidos en el SNCD.

1.2. Problema

Como se mencionó anteriormente, la obligatoriedad de brindar sus servicios de manera electrónica [1], ha provocado un aumento en la cantidad de entidades públicas que desarrollan o adquieren aplicaciones de software para la firma digital de documentos. Por ejemplo, el BCCR, la Contraloría de la República, el Poder Judicial, el Ministerio de Hacienda, Gobierno Digital, entre otras. Sin embargo, a pesar de que la Política de formatos oficiales de los documentos electrónicos firmados digitalmente establece que los formatos oficiales de firma son XAdES, CAdES y PAdES en su forma avanzada, la DCFD no provee una herramienta que permita verificar que los documentos que se están firmando tengan un formato válido.

Cada uno de los tres estándares establece varios perfiles de firma según el nivel de protección que se desee lograr, un perfil de firma se refiere a una serie de propiedades obligatorias y no obligatorias contenidas en una firma. Por ejemplo, el estándar XAdES define el perfil XAdES-BES para la firma básica de archivos XML, XAdES-T que agrega una propiedad de sello de tiempo para proveer el servicio de seguridad contra el no repudio, entre otros. El hecho de que no exista una herramienta oficial que permita verificar el formato de un

documento firmado puede provocar que las herramientas desarrolladas por las instituciones no estén firmando correctamente documentos, lo que podría generar problemas de validez de documentos firmados electrónicamente y de interoperabilidad entre las instituciones del estado.

Un problema de validez podría ser el siguiente: supongamos que el Ministerio X desarrolló un sistema que permite generar documentos firmados digitalmente en formato PDF. Y, a pesar de que se basa en el formato oficial avanzado XAdES para desarrollar el módulo de firma de PDF, olvida agregar la propiedad de listas de revocación de certificados (CRL). El sistema es puesto en marcha y los usuarios empiezan a generar documentos cuyas firmas están incompletas. Supongamos que un tiempo después la DCFD por medio del BCCR decide desarrollar una aplicación para validar documentos PDF firmados para resolver disputas legales, ya que ciudadanos han negado la autoría de documentos para evadir obligaciones. Los documentos generados con el sistema del Ministerio X no serían válidos, ya que no cumplen con el estándar oficial y esto pudo haberse evitado si esta entidad hubiese tenido un medio oficial para verificar que su aplicación estaba firmando correctamente.

Actualmente, no es posible garantizarles a las instituciones que sus aplicaciones firman documentos válidos dentro del SNCD, es por eso que es necesario proveerles un mecanismo que les dé esta garantía, ya sea poniendo a disposición una aplicación verificadora de formatos o por medio de un servicio de entidad certificadora que cuente con dicha aplicación para hacer la verificación.

1.3. Justificación

Como se explicó anteriormente, la firma digital en Costa Rica se ha extendido en los últimos años tanto en instituciones públicas como privadas, por su obligatoriedad desde hace cinco años (para las instituciones públicas) y por los grandes beneficios que provee.

Este aumento en la implementación de firma digital hace que sea aún más necesario identificar los perfiles de los formatos oficiales XAdES, CAdES y PAdES [3], que satisfagan los requerimientos técnicos y legales del SNCD para la firma digital de documentos electrónicos. A partir de la investigación y el análisis realizado en este trabajo, la DCFD podrá contar con documentación fundamentada técnicamente sobre los perfiles que se deben de estandarizar para la firma digital de documentos. Con la directriz de que todas las instituciones públicas deben de implementar la firma de digital, es de suma importancia que estos perfiles existan en forma de estándar, ya que pueden servir de guía para las instituciones públicas o privadas que deben o desean firmar digitalmente documentos y que deben de decidir entre desarrollar aplicaciones a la medida o adquirir paquetes de software para llevarlo a cabo. La no existencia de una normativa apropiada pone en riesgo tanto la validez de las aplicaciones como de los documentos firmados digitalmente en el SNCD.

Adicionalmente, este trabajo proporcionará a la DCFD una herramienta que servirá para determinar la validez del formato de firma de al menos uno de los formatos oficiales. La División de Servicios Tecnológicos del Banco Central de Costa Rica recomienda una serie de herramientas para firmar digitalmente un documento, pero no hace mención sobre alguna aplicación que permita la validación de los formatos de firma de los documentos. Esto le servirá de base a la DCFD para proporcionarle a las instituciones una herramienta que les ayude a determinar si el formato de un documento firmado es válido o no dentro del SNCD, es decir, si sus aplicaciones están funcionando correctamente para la firma de documentos.

Por lo tanto, este proyecto toma un valor doble de innovación, ya que se trata de firma digital, un tema novedoso en Costa Rica, y además provee una herramienta a la DCFD, actualmente inexistente, que podría brindar un mayor grado de robustez al SNCD en general. Por ejemplo, esta herramienta podría utilizarse en un futuro por alguna entidad certificadora de aplicaciones, que se encargue de definir si una aplicación que se va a utilizar en el SNCD de Costa Rica está firmando y/o validando correctamente los formatos oficiales de documentos.

1.4. Objetivos

El objetivo general de este TFIA fue desarrollar una aplicación de software para la validación de los formatos oficiales de firma digital dentro del Sistema Nacional de Certificación Digital de Costa Rica.

Los objetivos específicos durante el desarrollo de la investigación fueron:

- Identificar los perfiles legalmente válidos en Costa Rica para los formatos de firma digital XAdES, CAdES y PAdES.
- Seleccionar al menos un formato oficial y desarrollar una aplicación que permita validarlo.
- Validar la aplicación desarrollada desde el punto de vista funcional y de seguridad, en el marco de la legislación y regulaciones nacionales.

1.5. Alcance

Este trabajo se enfoca en la investigación de las leyes, reglamentos y políticas costarricenses sobre firma digital para identificar los perfiles oficiales de los formatos de firma digital de la ETSI XAdES, CAdES y PAdES.

Además, se desarrolla una herramienta que permite validar al menos uno de los formatos de firma propuestos. Para lograrlo se analizan los formatos y se selecciona uno de ellos con base en aspectos como: uso extendido en el país, herramientas disponibles para su manipulación y validación, documentación disponible en el SNCD sobre dicho formato, entre otros.

Para el desarrollo de esta aplicación, también se investiga sobre aplicaciones similares existentes y librerías de software utilizadas internacionalmente para el desarrollo de soluciones de firma digital, las cuales se utilizan como base para la obtención de requerimientos funcionales y de seguridad.

En resumen, con este trabajo se crea una herramienta que puede servir como base para una aplicación o servicio que brinde la DCFD para certificar que las aplicaciones de firma digital desarrolladas por instituciones públicas y privadas están firmando y generando documentos válidos dentro del SNCD.

1.6. Relevancia e impacto social

Con este trabajo se podrían ver beneficiados los siguientes actores del SNCD:

- La Dirección de Certificadores de Firma Digital.
- Instituciones públicas.
- Empresas privadas.
- Los usuarios finales.

Los resultados de esta investigación le permitirán a la DCFD contar con apoyo técnico en la valoración y definición de los perfiles oficiales de los formatos XAdES, CAdES y PAdES en el marco del SNCD.

Adicionalmente, la aplicación desarrollada servirá de base para la validación de los formatos de documentos firmados digitalmente en el SNCD. Esta aplicación podría ponerse a disposición de las instituciones públicas y empresas privadas que firman digitalmente documentos, para que puedan validar si lo están haciendo correctamente y sin poner en riesgo la validez legal de los mismos.

También, las personas físicas se podrían ver beneficiadas si la aplicación se pone a su disposición, ya que les podría dar seguridad sobre la validez de sus documentos firmados dentro del SNCD de Costa Rica.

1.7. Organización del documento

Este documento se organiza de la siguiente manera. El capítulo 2 brinda un resumen de conceptos básicos de seguridad, criptografía, PKI, estándares de firma digital y formatos de firma, necesarios para la comprensión de este documento. El capítulo 3, describe la metodología que se utilizó para este proyecto de investigación. El capítulo 4 presenta los resultados del proceso de identificación de los perfiles oficiales de firma digital en el SNCD. Se listan los perfiles oficiales, se evalúa su aplicabilidad en el país y se explica el proceso de selección de al menos uno para desarrollar la aplicación de validación. El capítulo 5 describe la aplicación desarrollada, sus componentes y los flujos de información. El capítulo 6 expone los resultados de las validaciones funcionales y de seguridad de la aplicación. Finalmente, el capítulo 7 resume las conclusiones obtenidas del trabajo realizado y detalla algunos elementos que pueden realizarse a futuro para continuar la investigación.

2. Marco Teórico

A continuación, se presenta un resumen de los principales conceptos relacionados con firma digital de documentos para una mejor comprensión de este trabajo de investigación. Se incluyen conceptos básicos de seguridad, criptografía, firma digital, infraestructura de llave pública y estándares de firma digital.

2.1. Conceptos básicos de la seguridad de la información

La seguridad de la información es un tema fundamental en las tecnologías de la computación y la informática. Su principal objetivo es proteger recursos valiosos para las organizaciones y personas como lo son la información, el *hardware* y el *software* [7].

Desafortunadamente, la seguridad de la información ha sido considerada un gasto innecesario por parte de algunas personas, gobiernos y organizaciones. Sin embargo, esta percepción ha ido cambiado con los años ante el crecimiento de la tecnología, la cantidad de amenazas que han surgido y las pérdidas económicas que se han presentado. Actualmente, existe una mayor conciencia sobre la importancia de proteger los recursos computacionales y la información. La seguridad de la información ha pasado de ser vista como un gasto innecesario a un medio para alcanzar los objetivos de las organizaciones y necesario para la protección de activos y personas.

2.1.1. Objetivos de seguridad

Los tres objetivos fundamentales de cualquier sistema de administración de la seguridad de la información son [7]:

- Confidencialidad
- Integridad
- Disponibilidad

La confidencialidad es la protección de la información dentro de los sistemas computacionales, de manera que personas, procesos y recursos no autorizados no puedan

acceder a dicha información. Los problemas de privacidad han recibido una mayor atención en los últimos años, lo cual enfatiza la importancia de la confidencialidad de la información por parte del gobierno y otras organizaciones [7].

La integridad consiste en la protección de la información o procesos de sistemas ante cualquier modificación no autorizada, ya sea de manera intencional o accidental. El reto de cualquier sistema de seguridad es asegurar que la información y los procesos se mantengan en el estado deseado a lo largo del tiempo. Para lograrlo es necesario no solo proteger la información sino también proteger los procesos o los medios utilizados para manipularla. Tanto la confidencialidad como la integridad dependen de mecanismos de control de acceso como la criptografía [7].

La disponibilidad se refiere al aseguramiento de que un recurso computacional esté accesible en el momento que sea necesario por usuarios autorizados [7].

Existen otros objetivos de seguridad dependiendo de la naturaleza del sistema que se desee proteger. En el caso de una infraestructura de llave pública, como la firma digital, tres objetivos fundamentales son [8]:

- Autenticación
- Autenticidad
- No repudio

La autenticación es un proceso por el cual un verificador puede estar seguro sobre la identidad de una persona o sistema. La autenticidad es la capacidad de poder determinar el origen y la veracidad de la información. El no repudio es una característica de la información que evita que una persona o ente niegue su autoría sobre la información o sobre una acción [8].

2.1.2. Amenazas

Las amenazas son una posible violación a la seguridad de un sistema. Las amenazas están siempre presentes, no necesariamente se tiene que dar una violación a la seguridad para considerar que existe una amenaza. En la **Tabla 1** se muestran algunos tipos de amenazas.

Tabla 1. Tipos de amenazas [9].

Nombre	Descripción
Divulgación (*disclosure*)	Es el acceso no autorizado a la información.
Engaño (*deception*)	Es la aceptación de datos falsos.
Interrupción (*disruption*)	Es la prevención de una operación correcta.
Usurpación (*usurpation*)	Es el control no autorizado de alguna parte de un sistema.

Algunas de las amenazas que pertenecen a estos grupos y que vale la pena mencionar, ya que se relacionan con el problema que se desea resolver son [10]:

- Intromisión (*snooping*): es la interceptación de información de forma no autorizada. Es una forma de divulgación. Un ejemplo de este tipo de amenaza es el *Wiretapping*, cuyo ataque consiste en monitorear una red. Los servicios de confidencialidad buscan contrarrestar esta amenaza.
- Modificación (*modification*): es un cambio no autorizado de información. Puede ser una forma de engaño, donde una entidad confía en datos incorrectos. También puede ser una forma de interrupción y usurpación. El *Active Wiretapping* es una forma de modificación de datos de transitan en una red. Un ejemplo de este tipo de ataques es el *man-in-the-middle* en el cual se interceptan mensajes enviados por un remitente y se modifican para enviarle mensajes modificados al destinatario sin que ninguno se dé cuenta de la presencia del atacante. Los servicios de integridad contrarrestan esta amenaza.
- Enmascaramiento (*spoofing*): es la impersonalización de una entidad por otra. Es una forma de engaño y usurpación. Por ejemplo, cuando una entidad quiere acceder a un archivo y un atacante lo cambia por otro de forma activa, es decir, en el momento del acceso. Los servicios de integridad contrarrestan esta amenaza.
- Repudio de origen (*repudiation of origin*): es una negación falsa de que una entidad envió o creo algo. Es una forma de engaño. Por ejemplo, cuando una entidad niega haber creado un documento y por ende la información que este contiene, el ataque se

considera exitoso cuando no hay manera de comprobar que la entidad creó el documento. Mecanismos de integridad contrarrestan esta amenaza.

- Negación de recibido (*denial of receipt*): es cuando una entidad niega haber recibido alguna información. Es una forma de engaño. Los servicios de integridad y disponibilidad contrarrestan esta amenaza.
- Retraso de servicio (*delay*): es la inhibición del servicio durante un tiempo corto. Es una forma de usurpación y de engaño. Este tipo de ataques pueden ocurrir en el origen, en el destino o en el medio de la comunicación. Los servicios de disponibilidad contrarrestan esta amenaza.
- Negación de servicio (*denial of service*): es la inhibición del servicio durante un tiempo prolongado. Es una forma de usurpación y de engaño. Este tipo de ataques pueden ocurrir en el origen, en el destino o en el medio de la comunicación. Los servicios de disponibilidad contrarrestan esta amenaza.

Para contrarrestar las amenazas se deben de reforzar los objetivos de seguridad mencionados anteriormente con políticas y mecanismos de seguridad.

2.1.3. Políticas y mecanismos de seguridad

Una política es una declaración de lo que está permitido y de lo que no. La imposición de diferentes políticas de seguridad va a depender de la naturaleza del sistema, de las amenazas a las que se está expuesto, los recursos disponibles y la información que se maneja [10].

Por otro lado, un mecanismo de seguridad es un método, herramienta o procedimiento que permite cumplir con una política de seguridad [10]. Un mecanismo puede ser técnico o no técnico. Un ejemplo de un mecanismo no técnico es cuando una empresa u organización requiere que sus empleados se identifiquen a la hora de entrar al edificio. Un ejemplo de un mecanismo de seguridad técnico es la criptografía, la cual, como se explica en la siguiente sección, sirve para proteger la integridad y la confidencialidad de la información.

2.2. Criptografía

Debido a que la criptografía es un tema matemático bastante profundo y que para efectos de este proyecto la criptografía es vista como una herramienta de soporte para lograr los objetivos, solamente se presentan generalidades sobre este tema.

La palabra criptografía proviene del griego "escritura secreta" ("*secret writing"*) [10] y es un mecanismo de seguridad que busca mantener privados los mensajes entre dos entidades (personas o equipos). Esto se logra por medio de funciones de cifrado que modifican el mensaje original de manera que no sea legible por entidades que no estén autorizadas a ver el mensaje y solamente el destinatario del mensaje puede ver el mensaje por medio de funciones de descifrado del mensaje. Estas funciones pueden utilizar llaves privadas (solamente las entidades las conocen), públicas (cualquier entidad la conoce) o ambas para cifrar y descifrar el mensaje, respectivamente. A los conjuntos de funciones de cifrado y descifrado se les conoce como algoritmo de cifrado.

El componente básico de la criptografía es un sistema criptográfico definido como una quíntupla (E, D, M, K, C), en donde [10]:

M = { un conjunto de textos planos }

K = { un conjunto de llaves }

C = { un conjunto de textos cifrados }

E = { es el conjunto de funciones de cifrado (E: M x K → C) }

D = { es el conjunto de funciones de descifrado (D: C x K → M) }

En general, la criptografía tiene varios objetivos que se relacionan directamente con los servicios de seguridad. Tiene el objetivo de mantener privado un mensaje, es decir, mantener la confidencialidad del mensaje. También, tiene el objetivo de proteger el mensaje de cualquier modificación para mantener la integridad del mismo. Además, los sistemas criptográficos modernos, como la criptografía de llave pública, permiten identificar el remitente del mensaje, es decir, permiten brindar los servicios de autenticación y no repudio.

A continuación, se presentan algunos de los sistemas criptográficos, los cuales se dividen en sistemas criptográficos clásicos y sistemas criptográficos de llave pública.

2.2.1. Sistemas criptográficos clásicos

Son sistemas criptográficos que utilizan la misma llave tanto para el cifrado como para el descifrado (ver **Figura 1**). Se les conoce como sistemas simétricos o *single-key* y se pueden clasificar en cifrados de transposición, de sustitución y de producto [10].

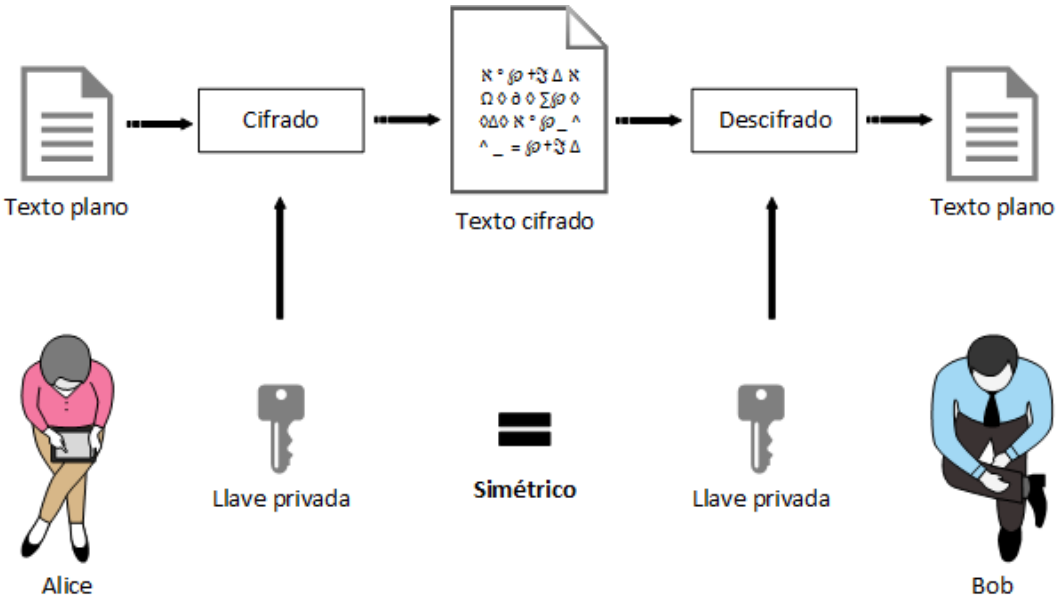

Figura 1. Cifrado Simétrico. Tomado de [8].

Un cifrado de transposición reorganiza los caracteres de un texto plano para generar el texto cifrado y las letras que lo componen no son cambiadas. Por otro lado, un cifrado de sustitución cambia las letras que componen el texto plano para generar el texto cifrado. Por último, un cifrado de producto combina las técnicas de transposición y de sustitución, y se diferencia de los otros en que realiza estas operaciones a nivel de bits. Un ejemplo de este tipo de cifrado es el *Data Encryption Standard* (DES).

2.2.2. Sistemas criptográficos de llave pública

Los sistemas criptográficos de llave pública utilizan una llave para cifrado y una diferente para el descifrado (ver **Figura 2**). Este esquema fue propuesto por Diffie y Hellman en 1976 [10].

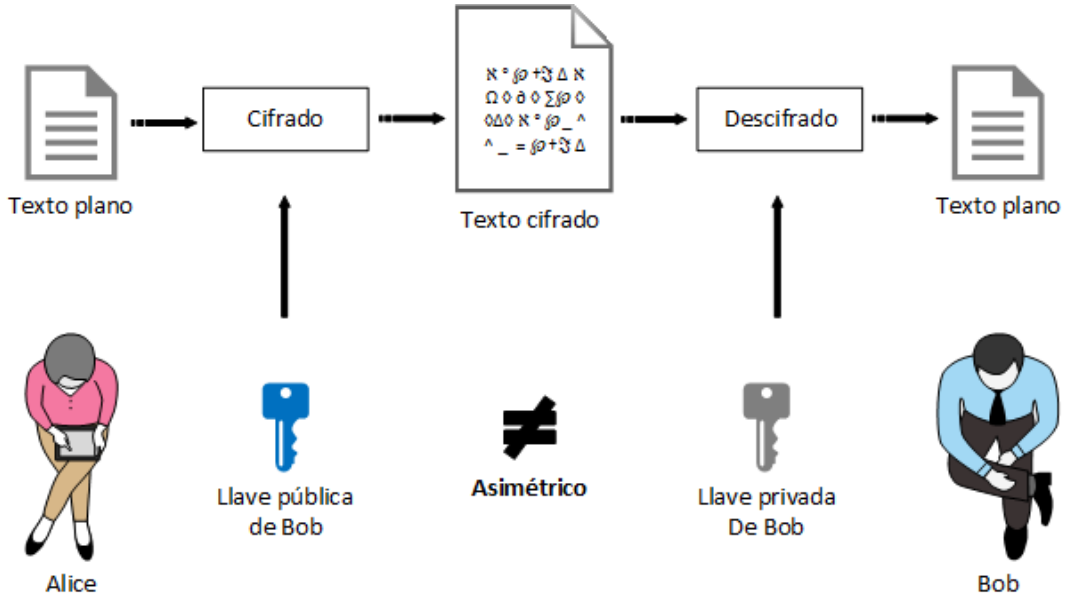

Figura 2. Cifrado Asimétrico. Tomado de [8].

En la siguiente sección se brindan más detalles sobre la criptografía de llave pública y los servicios de seguridad que provee.

2.3. Criptografía de llave pública

Una forma de criptografía es la criptografía de llave pública. En este tipo de criptografía se utilizan dos llaves distintas pero relacionadas al receptor del mensaje: una pública para cifrar el mensaje y una privada para descifrar el mensaje (ver **Figura 2**). Una característica importante de estas llaves es que la llave privada no puede ser calculada o inferida con la llave pública [8].

Todo sistema criptográfico de llave pública debe cumplir con las siguientes condiciones [10]:

1. Cifrar y descifrar el mensaje, dada la llave correspondiente, debe de ser computacionalmente sencillo.
2. Inferir la llave privada de la llave pública debe de ser computacionalmente inviable.
3. Determinar la llave privada a partir del texto cifrado debe de ser computacionalmente inviable.

Este tipo de criptografía proporciona los siguientes servicios de seguridad [8]:

- Confidencialidad: ya que sólo es posible ver el mensaje original al descifrarlo con la llave privada correspondiente a la llave pública utilizada para cifrar el mensaje, y solamente el receptor la conoce.
- Integridad: el mensaje original sólo puede ser modificado si es descifrado previamente.
- Autenticación: por ejemplo, una entidad verificadora puede solicitarle a una entidad que se desee autenticar que dado un mensaje cifrado por la entidad verificadora (con una llave pública) sea descifrado por la entidad con la llave privada correspondiente, posteriormente la entidad verificadora puede comparar el mensaje original con el descifrado por la entidad y si son iguales la autenticación es exitosa. Sin embargo, esto tiene potenciales problemas de seguridad, por lo que para este servicio de seguridad se utiliza la firma digital [8], mecanismo cuyo sistema criptográfico base es el cifrado de llave pública.

A los sistemas criptográficos de llave pública también se les conoce como sistemas criptográficos asimétricos. Algunos ejemplos de estos sistemas son el de Diffie-Hellman, RSA y Firma Digital [10].

2.4. Algoritmo Hash

El algoritmo *hash* es una función mediante la cual se realiza un mapeo de un conjunto de datos (bits) a otro conjunto de datos normalmente más pequeño, al cual se le llama resumen o *digest* [8].

Un algoritmo hash debe tener ciertas características:

1. Debe de ser libre de colisiones, es decir, que no debe de existir dos conjuntos de datos distintos que generen el mismo *digest*.
2. Debe de ser referencialmente transparente, lo cual, quiere decir que dos ejecuciones distintas del algoritmo con el mismo conjunto de datos de entrada deben producir el mismo *digest*.
3. Los *digest* que se generen con el algoritmo tienen que ser de un tamaño fijo.
4. Debe de ser de una sola dirección, es decir, que no debe de ser posible reconstruir el conjunto de datos original a partir del *digest*.

Las funciones hash se utilizan para proveer el servicio de integridad [8]. Por ejemplo, cuando se instala un determinado software, una vez instalado se puede calcular el *hash* o *digest* para utilizarlo en un futuro para verificar si el software ha sido modificado o no.

Los algoritmos *hash* son, junto con la criptografía de llave pública, la base de la firma digital. En la siguiente sección se explica cómo estas herramientas se utilizan para generar una firma digital.

2.5. Firma digital

La criptografía de llave pública es la base de la firma digital. En este esquema un firmante utiliza su llave de firma para generar firmas digitales a partir de documentos. Esta llave se denomina llave privada. Posteriormente, potenciales verificadores podrían usar la llave de verificación del firmante que corresponde a la llave privada para validar la firma digital. Esta llave se llama llave pública [8].

Sin embargo, en la práctica la firma digital no se calcula sobre el documento original, sino que se utiliza un algoritmo *hash* para generar un *digest* o resumen del documento y sobre este resumen se genera la firma.

En la **Figura 3** se muestra el proceso de firma digital entre Alice y Bob.

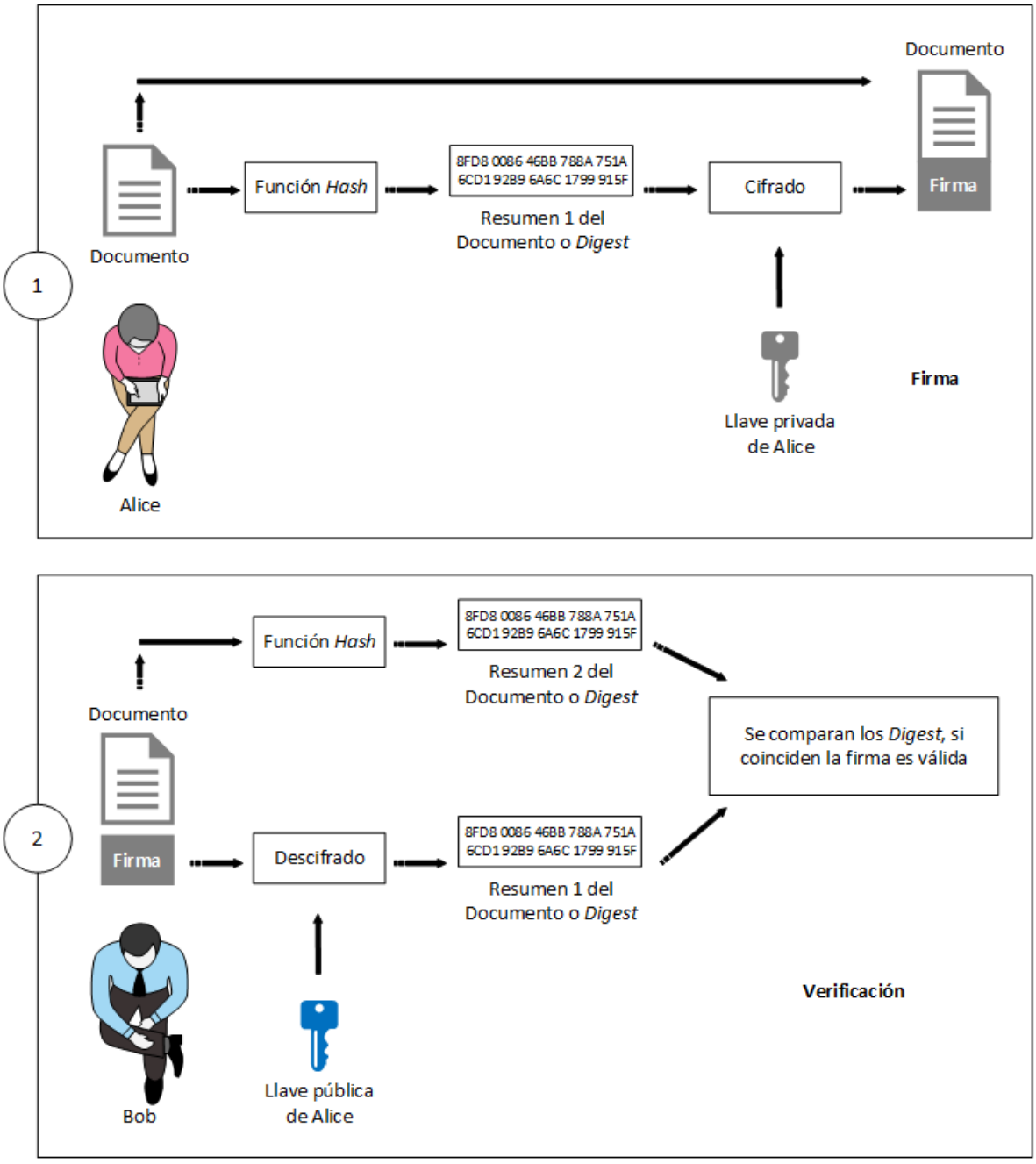

Figura 3. Proceso de Firma Digital. Tomado de [8].

La firma digital es un mecanismo de seguridad muy importante en las tecnologías de la información, ya que provee los siguientes servicios de seguridad:

- Integridad
- Autenticidad
- Autenticación
- No repudio

Por ejemplo, tomando como base la **Figura 3**, si Alice firma digitalmente una transacción bancaria y posteriormente Bob verifica la firma, él podría convencerse de que la que originó la transacción fue Alice y que la información no ha sido alterada. De esta manera se establece la integridad y autenticidad de la información.

Por otro lado, supongamos que Alice y Bob inician una relación contractual. Ambos firman el contrato digitalmente. Y en un futuro Bob niega haber firmado el contrato. Entonces, Alice presenta la firma digital de Bob frente a la instancia judicial correspondiente para probar que Bob efectivamente si firmó el documento. El juez obtiene la llave pública de Bob y verifica la firma, esto convence al juez de que Bob si firmó el contrato. Por lo tanto, la firma digital también provee el servicio de no repudio de la información.

También, la firma digital provee el servicio de autenticación. Supongamos que Alice se desea identificar con Bob. Bob envía un número aleatorio a Alice. Ella firma este número y envía a Bob la firma digital. La verificación exitosa de la firma convence a Bob de la identidad de Alice.

2.6. Infraestructura de llave pública

La firma digital y en general los sistemas criptográficos de llave pública permiten alcanzar importantes servicios de seguridad. Sin embargo, estos sistemas requieren de una correcta administración de las llaves durante todo su ciclo de vida, desde la generación de las llaves, durante su uso y hasta que el par de llaves (pública y privada) sean invalidadas. Las llaves pueden ser invalidadas porque expiraron o porque han sido comprometidas.

La infraestructura de llave pública o PKI (por las siglas en inglés), tiene como propósito proveer una correcta administración de las llaves. A continuación, se presentan cada una de las tareas de una infraestructura de llave pública asociada con cada etapa del ciclo de vida de un par de llaves [8]:

- En la fase de generación de llaves, debe asegurar que se produzca un par de llaves seguras. Esta tarea es bastante compleja para PKI, ya que la entidad que produzca las llaves debe de tener la capacidad técnica para lograrlo, pero también debe garantizar que la llave privada solo la conozca su dueño para garantizar la confidencialidad.
- Durante la fase de uso de las llaves, debe poner a disponibilidad de los usuarios las llaves públicas cuando lo requieran. Esta es la tarea más importante y compleja de una PKI. Esto porque no basta con hacerlas accesibles al público, sino que los usuarios deben tener la posibilidad de acceder a sus propiedades y de verificar la autenticidad y validez de las llaves.
- Si un par de llaves se vuelve inseguro durante su fase de uso, PKI debe informar a los usuarios de esta situación. También, si el sistema criptográfico que se utilizó para generar las llaves a sido quebrado, todas las llaves generadas con ese sistema deben ser invalidadas.
- Otra tarea de PKI durante el uso de las llaves es la de permitir respaldar las llaves. Esta tarea es muy sensible, ya que no deben de existir respaldos de llaves privadas. Es probable que en caso de pérdida de una llave privada se deban generar un nuevo par de llaves.
- En general, durante la fase de uso de las llaves privadas, PKI debe proveer un medio para almacenarlas y accederlas. Por ejemplo, con el uso de tarjetas inteligentes (*smart cards*).
- Finalmente, una vez que un par de llaves expire o sea invalidado por alguna razón, PKI debe administrarlas correctamente. Por ejemplo, debe destruirlas o archivarlas para referencias futuras y así poder proveer autenticación y no repudio a largo plazo.

En una PKI se definen los siguientes componentes que se mencionan a continuación [8]:

- Certificados Digitales
- Listas de Revocación de Certificados
- Protocolo de Estado del Certificado en Línea
- Usuarios Finales
- Autoridades Certificadoras
- Autoridades de Registro
- Dispositivo Criptográfico
- Repositorios
- Sellado de Tiempo

2.6.1. Certificados digitales

Anteriormente, se mencionó que una de las mayores tareas de una PKI es proveer pruebas de autenticidad de las llaves públicas. Los certificados digitales son herramientas que se utilizan para brindar dichas pruebas.

Los certificados digitales son estructuras de datos que relacionan llaves públicas con entidades y que son firmados por un tercero. Los certificados permiten reducir la confianza en una llave pública de una entidad para confiar en una autoridad, la que firma el certificado de la entidad. Por medio de la firma del certificado, la autoridad está certificando que efectivamente la llave pública pertenece a la entidad [8].

Un certificado debe tener como mínimo los siguientes datos:

1. El nombre de la entidad a la que pertenece la llave pública.
2. La llave pública.
3. El algoritmo criptográfico que se debe utilizar con la llave pública.
4. El número de serie del certificado.
5. El periodo de validez del certificado.
6. El nombre de la autoridad que generó y firmó el certificado.
7. Restricciones sobre el uso de la llave pública en el certificado.

El contenido del certificado es firmado por la autoridad que lo generó y la firma normalmente

se agrega al certificado junto con el algoritmo utilizado para generar dicha firma. El estándar más importante sobre el formato de un certificado de llave pública es el X.509, en la **Tabla 2** se muestran los campos de un certificado de este tipo en la versión 3.

Tabla 2. Campos de un certificado v3 [8].

Elemento	Campo

Certificado	• Versión
	• Número de serie
	• Id del algoritmo
	• Editor
	• Periodo de validez
	  o No antes
	  o No después
	• Nombre del sujeto
	• Información de Llave Pública del sujeto
	  o Algoritmo de llave pública
	  o Llave pública
	• Identificador del Editor (opcional)
	• Identificador del Sujeto (opcional)
	• Extensiones (opcional)
	  o Identificador de la llave de la autoridad certificadora.
	  o Identificador de la llave del sujeto.
	  o Uso de la llave
	  o Usos extendidos de la llave
	  o Puntos de distribución de CRL
	  o Otros

Firma del certificado	La firma generada a partir de los campos del certificado.
Algoritmo de firma del certificado	El algoritmo utilizado para la generación de la firma. El más común es SHA1 con RSA

2.6.2. Listas de Revocación de Certificados

La Lista de Revocación de Certificados (CRL por sus siglas en inglés), es el mecanismo utilizado en una PKI para publicar información de revocación de certificados. Una CRL es

la lista de certificados revocados, la cual también es firmada digitalmente para probar su autenticidad [8].

La CRL es actualizada regularmente y cualquier usuario que la desee acceder debe descargarla para posteriormente verificar la firma digital.

2.6.3. Protocolo de Estado del Certificado en Línea

Debido a que la CRL puede llegar a ser muy grande y a que puede no estar actualizada por el tiempo entre actualizaciones, se inventó el protocolo Protocolo de Estado del Certificado en Línea (OCSP por sus siglas en inglés). Este protocolo permite a los clientes consultar un servidor de OCSP sobre el estado de un certificado en específico [8].

Algunas ventajas de OCSP sobre la CRL son:

- siempre se puede obtener información actualizada sobre el estado de revocación de un certificado.
- no requiere mucho espacio de almacenamiento, solo para almacenar el certificado que se está validando.

2.6.4. Usuarios Finales

Los usuarios finales de una PKI son aquellas entidades, personas, servidores o dispositivos que se registran para obtener certificados digitales que los identifiquen y así poder realizar transacciones.

2.6.5. Autoridades Certificadoras

Una Autoridad Certificadora (CA por sus siglas en inglés) en una PKI es la entidad encargada de emitir los certificados de llave pública a los usuarios. Además, se encarga de certificar la autenticidad de las llaves públicas que brinda, por lo que su certificado digital siempre debe de estar disponible y de fácil acceso [8].

También, la CA debe mantener al día la información de los estados de los certificados, la CRL, los certificados revocados y debe de mantener en archivo los certificados que han expirados o han sido revocados para referencias futuras.

2.6.6. Autoridades de registro

Las Autoridades de Registro (RA por sus siglas en inglés), es la entidad encargada de registrar los usuarios en la PKI. Además, valida que la información del usuario corresponda realmente a la entidad que solicita el ingreso a la PKI antes de que la CA emita el certificado y las llaves públicas.

2.6.7. Dispositivo Criptográfico

Se refiere al medio físico donde se generan, almacenan y protegen las llaves criptográficas, tanto públicas como privadas. Por ejemplo, la llave privada del cliente se genera en un dispositivo especial que la almacena en otro dispositivo, como una smart card, el cual tiene protección por medio de PIN para poder acceder a dicha llave privada.

2.6.8. Repositorios

Lo repositorios son medio de almacenamiento donde se guardan los certificados de llave pública de la CA y las CRLs. También, deben permitir acceder a la información en un momento dado para validar la veracidad de un certificado digital.

2.6.9. Sellado de Tiempo

Es el proceso que certifica, mediante un sello de tiempo, que un conjunto de datos existió en un momento determinado y que esos datos no han sido modificados. Por ejemplo, para validar que un documento fue firmado digitalmente antes de que el certificado digital correspondiente fuera revocado. Un sello de tiempo es una secuencia de caracteres sobre la fecha y hora en la que se presentó un evento [8].

Dentro de la PKI, existe una entidad llamada Autoridad de Sellado de Tiempo (TSA por sus siglas en inglés) que se encarga de ofrecer los servicios de sellado de tiempo. Esta entidad es un tercero de confianza que brinda una estampa de tiempo confiable para que sea agregada a la firma.

2.7. Estándares de firma digital

Un estándar es un documento establecido por consenso y aprobado por un organismo reconocido que provee reglas, guías o características para la realización de actividades comunes y de uso repetitivo, el cual está orientado a mantener y maximizar el orden en un contexto dado [11]. A este documento se le asigna un nombre según su contenido, estructura y autores. De igual manera, un estándar de firma digital es una especificación dada por una organización reconocida que define la estructura que debe cumplir un documento firmado digitalmente.

En una PKI donde se realice la firma digital de documentos es fundamental que exista un estándar o un conjunto de estándares para los documentos firmados digitalmente. De lo contrario, sería imposible validar los documentos y su firma, dada la gran variedad de estándares y formatos existentes.

Algunas de las organizaciones más reconocidas a nivel mundial que establecen estándares en el campo de la firma digital son:

2.7.1. Organización Internacional de Estándares (ISO)

Es la organización más grande a nivel mundial dedicada al desarrollo y publicación de estándares internacionales. Es una organización no gubernamental que contempla los requerimientos de los negocios y las necesidades de las personas para establecer una solución a un problema dado [11].

2.7.2. Instituto Europeo de Estándares y Telecomunicaciones (ETSI)

Es una organización de estándares europeos reconocida como tal por la Unión Europea (EU por sus siglas en inglés). Produce estándares aplicables a nivel mundial para las tecnologías de la información y comunicación. Los documentos de especificación que desarrolla, se utilizan cuando los datos que contienen son requerimientos normativos y cuando es necesario el mantenimiento, la validación y la rápida difusión [12].

2.8. Formatos de firma digital

Los formatos de firma digital son especificaciones donde se define la estructura de un documento firmado digitalmente y que son aplicables a diferentes tipos de archivos. Por ejemplo, se puede definir un formato para la firma de un documento XML el cual es diferente a un formato para la firma de un documento de PDF, ya que la estructura de los archivos es distinta.

La ETSI, por ejemplo, define diferentes formatos de firma según el tipo de archivo que se desee firmar digitalmente:

- **CAdES** (CMS Avanzado): Es la evolución del primer formato de firma estandarizado. Es apropiado para firmar archivos grandes, especialmente si la firma contiene el documento original porque optimiza el espacio de la información. Tras firmar, no es posible ver la información firmada, porque la información se guarda de forma binaria. [13]

- **XAdES** (XML Avanzado): El resultado es un archivo de texto XML. Los documentos obtenidos suelen ser más grandes que en el caso de CAdES, por eso no es adecuado cuando el archivo original es muy grande. [14]

- **PAdES** (PDF Avanzado): Este es el formato más adecuado cuando el documento original es un PDF. El destinatario de la firma puede comprobar fácilmente la firma y el documento firmado utilizando Adobe Reader. [15]

2.9. Perfiles de firma digital

Si bien un estándar de firma digital define la estructura o formato que debe tener un documento firmado digitalmente, es posible que en dicho formato se incluyan atributos opcionales que se pueden incorporar a la firma digital, dando como resultado un formato flexible y adaptable a diferentes requerimientos técnicos. A estos formatos flexibles generados a partir de una estructura en común se les denomina perfiles de firma digital [12].

En el marco teórico presentado se incluyeron los principales conceptos relacionados con la firma digital de documentos para permitir una mejor comprensión de este trabajo de investigación. En los siguientes capítulos, se describe la metodología y posteriormente se presentan los resultados obtenidos durante esta investigación.

3. Metodología

En este capítulo se presenta la metodología seleccionada para cumplir con los objetivos definidos en esta investigación y se describe cada una de las etapas que la componen. Se inicia con la identificación de los perfiles de firma digital de documentos que son considerados válidos según la legislación vigente en Costa Rica. Luego, se evalúa si cumplen los requerimientos técnicos de firma digital dentro del SNCD. Después, se selecciona al menos uno de los perfiles para desarrollar una aplicación que permita validarlo. Posteriormente, se desarrolla la aplicación y, finalmente, se valida desde el punto de vista funcional y de seguridad. Este proceso se muestra en la **Figura 4**.

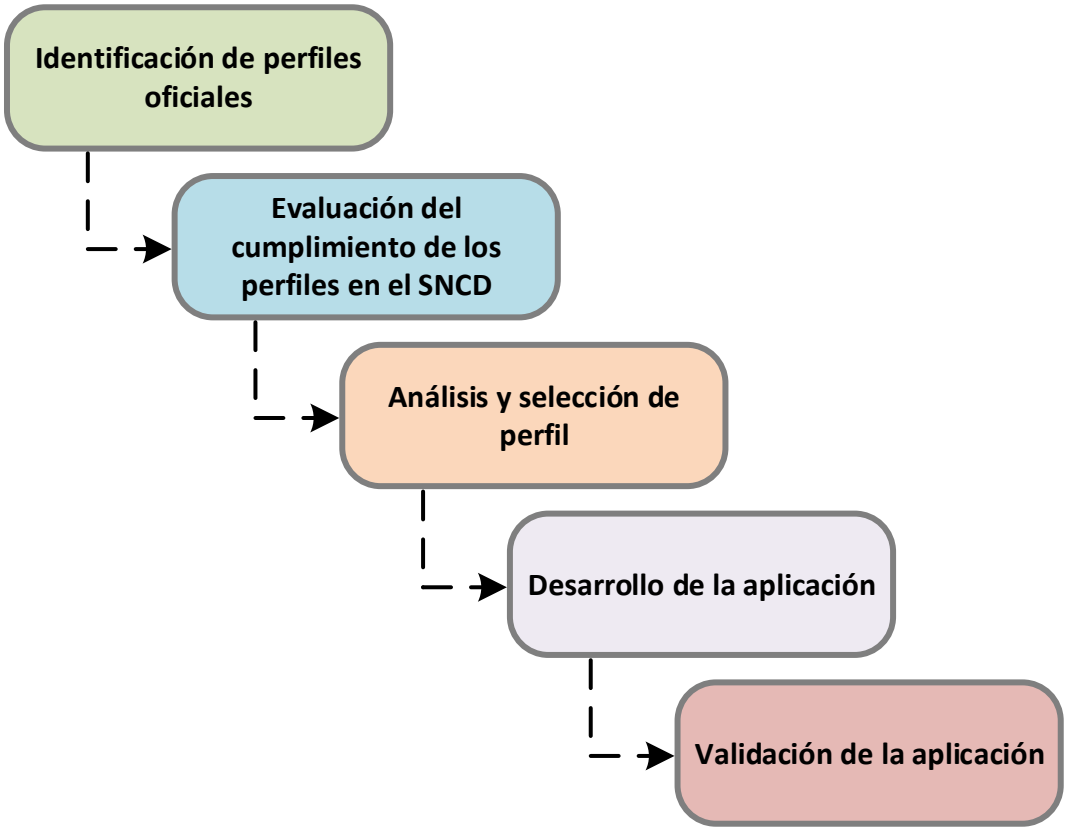

Figura 4. Metodología del proyecto

3.1. Identificación de perfiles oficiales

Para la identificación de los perfiles de firma digital legalmente válidos dentro del SNCD se realizó una revisión sistemática de los documentos oficiales sobre firma digital distribuidos por el Gobierno de Costa Rica. Estos documentos se obtuvieron del sitio web oficial www.firmadigital.go.cr del MICITT:

- *Ley de certificados, firmas digitales y documentos electrónicos Nº 8454.*
- *Reglamento a la ley de certificados, firmas digitales y documentos electrónicos.*
- *Política de formatos oficiales de los documentos electrónicos firmados digitalmente.*

En la **Figura 5** se muestra que el primer documento que se revisó fue la Ley 8454 como base legal de la firma digital en el país. Posteriormente, se consultó el reglamento a la Ley. Y finalmente, se examinó la política de los formatos oficiales.

Una vez que se lograron identificar los perfiles oficiales, se estudiaron los estándares sobre los perfiles con el fin de poder explicarlos en el presente documento.

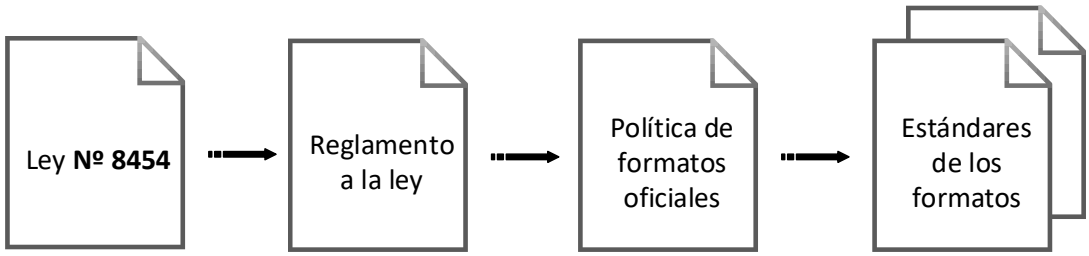

Figura 5. Metodología para la identificación de los estándares y perfiles oficiales de firma digital.

3.2. Valoración del cumplimiento de los perfiles en el SNCD

Con los perfiles oficiales identificados, se procedió a valorar si la especificación técnica de los perfiles cumple con los requerimientos de firma digital establecidos en la regulación del SNCD. Para lograrlo, primero se realizó una revisión estructurada de la ley de firma digital, el reglamento a la ley y las políticas para identificar los requerimientos técnicos para la firma digital de documentos. Luego se analizaron los estándares de los formatos para poder caracterizarlos. Con base en los resultados obtenidos, se realizó un control cruzado, verificando cada uno de los elementos técnicos que son requeridos contra las características de los perfiles, para determinar si cumplen con los requisitos a nivel país para la firma digital de documentos. Y en el caso de que no los cumplan, realizar recomendaciones como parte de este proyecto sobre cuáles son los perfiles más adecuados. Estas recomendaciones podrían ser consideradas eventualmente por las entidades encargadas de la implementación de firma digital en el país.

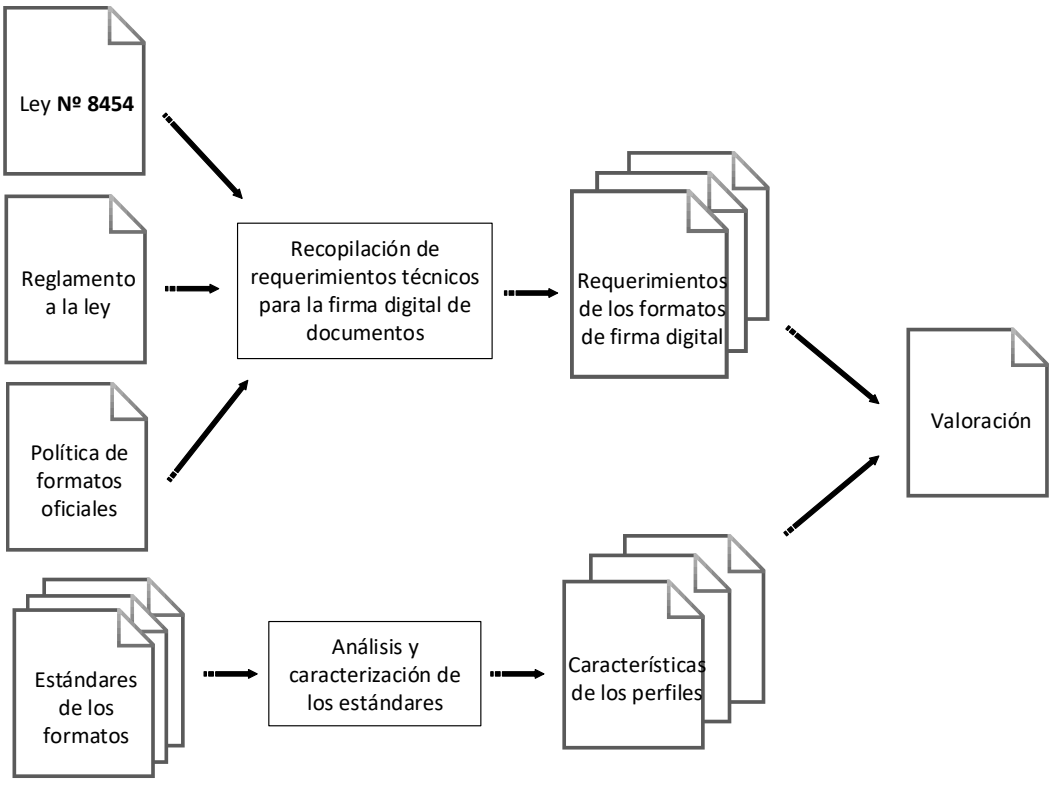

Figura 6. Proceso de valoración del cumplimiento de los perfiles en el SNCD.

3.3. Análisis de los formatos y selección de al menos uno para ser validado por la aplicación

La selección de al menos uno de los formatos para validarlo con la aplicación que se desea desarrollar no puede ser arbitraria. Es necesario realizar un análisis de cada uno de los formatos con el fin de caracterizarlos y utilizar las características obtenidas como criterios de selección.

Por lo tanto, inicialmente fue necesario revisar los estándares para extraer las características más importantes de cada uno. Algunos ejemplos de las características extraídas son:

- El tipo de archivo que permite firmar el estándar (XML, PDF o binario).
- El tipo de firma (si es desacoplada, encapsulada o encapsuladora)
- Si requiere de alguno de los otros estándares para generar la firma

Luego, partir de estas se obtuvieron más características, por ejemplo:

- El nivel de complejidad de desarrollo.
- El tiempo estimado de desarrollo.
- Si existen herramientas o librerías que puedan ser utilizadas en el desarrollo.
- La importancia y el uso de los tipos de documentos en el país.

Finalmente, se realizó un análisis de los datos obtenidos para tomar una decisión fundamentada, sobre el formato a validar con la aplicación. En la **Figura 7** se muestra el proceso llevado a cabo.

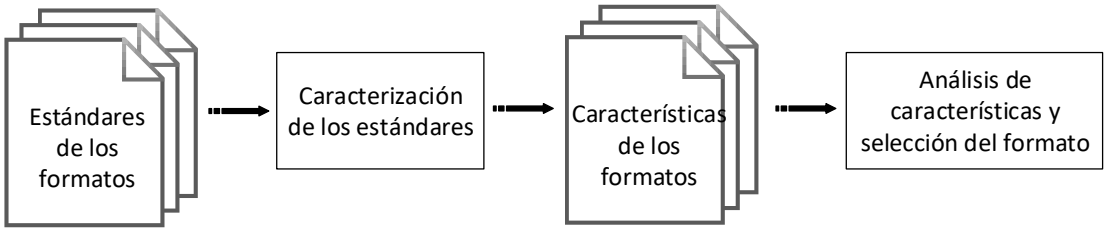

Figura 7. Metodología para la selección del formato para ser validado con la aplicación.

3.4. Desarrollo de la aplicación

Para desarrollar la aplicación se utilizó la metodología que se presenta en la **Figura 8**.

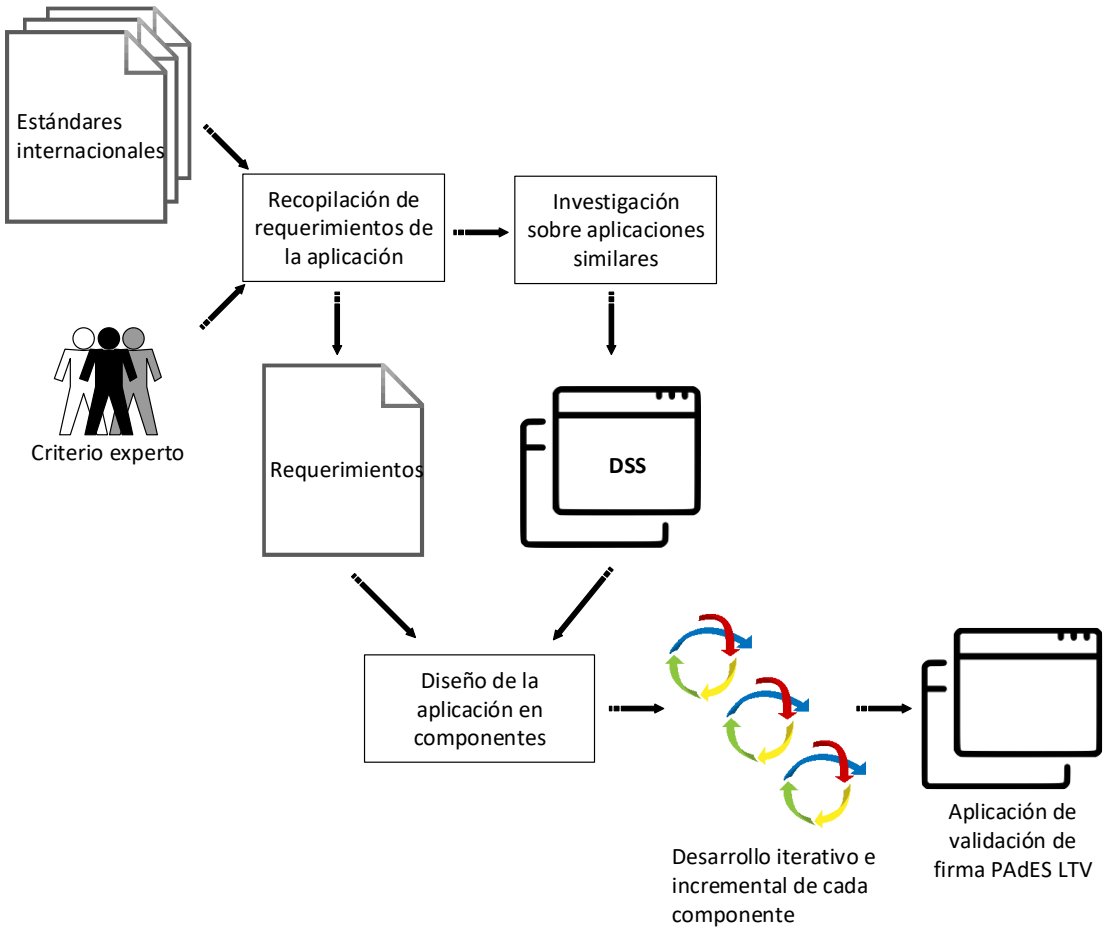

Figura 8. Metodología de desarrollo de la aplicación.

Primero fue necesario consultar fuentes de información que permitieran recopilar los requerimientos de la aplicación para validar correctamente el formato de firma seleccionado. Las fuentes consultadas fueron:

- Estándares internacionales.
- Criterio experto de integrantes del BCCR y del MICITT.

Una revisión sistemática de los estándares internacionales, permitió recopilar todos los requerimientos funcionales de la aplicación, así como los requerimientos arquitectónicos.

Para definir aspectos tecnológicos de la aplicación, como el lenguaje de programación y las librerías de terceros para realizar tareas específicas, se consultó a expertos del BCCR y del MICITT involucrados en el tema de firma digital. Se estableció que el lenguaje de programación debía de ser C# del marco de trabajo .NET de Microsoft. También, se definió que las librerías BouncyCastle y iTextSharp se debían de utilizar para el manejo de la criptografía y de los archivos PDF, respectivamente.

Luego, con los requerimientos funcionales, arquitectónicos y tecnológicos definidos, se procedió a investigar sobre implementaciones similares a nivel internacional que pudieran ser utilizadas de ejemplo. Para esto se realizaron diferentes consultas web por medio del motor de búsqueda de Google. Se consultó sobre gobiernos u organizaciones que estuvieran utilizando los estándares de la ETSI como formatos oficiales de firma y sobre aplicaciones que permitieran validarlos. Por medio de estas consultas se logró determinar que la Unión Europea tiene a disposición de los países miembros, una librería para la firma y validación de firma digital denominada Digital Signature Service (DSS) [16]. Esta es una librería de código abierto escrita en el lenguaje de programación Java, desarrollada con base en los estándares de la ETSI y que permite firmar y validar los formatos AdES. Estos estándares son los oficiales para la Unión Europea.

Finalmente, se procedió al desarrollo de la aplicación utilizando como insumos los requerimientos recopilados y la librería DSS de la Unión Europea. Para lograrlo, se utilizó una estrategia de desarrollo ágil e incremental, en dónde la funcionalidad requerida se dividió en componentes que se construyeron de forma separada y progresivamente en iteraciones, para integrarlos posteriormente. Esto facilitó las pruebas de desarrollo, ya que cada componente se probó individualmente conforme se iba desarrollando y no al final, como en modelos tradicionales. Parte de este proceso consistió en la migración de los componentes de la librería DSS al lenguaje C#. Estos componentes se adaptaron a las tecnologías establecidas y se verificaron con los requerimientos recopilados. Este proceso de adaptación

fue requerido porque algunas de las librerías de terceros utilizadas por los componentes de DSS no están disponibles para el lenguaje C#. Por ejemplo, DSS utiliza PdfBox para manipular archivos PDF, pero esta librería solo existe para el lenguaje Java, por lo que se tuvo que adaptar la funcionalidad a la librería iTextSharp de C# .NET.

En cada iteración de la estrategia de desarrollo se realizaron las siguientes actividades:

- **Descubrimiento**: Identificación del componente a desarrollar. Por medio de la revisión de la librería DSS y de los requerimientos.
- **Diseño**: diseño del componente basándose en los requerimientos y en la librería DSS.
- **Investigación**: investigación sobre cómo utilizar las librerías de terceros. Solamente en caso de ser requerida.
- **Desarrollo**: creación o migración de la funcionalidad de la librería DSS.
- **Pruebas**: ejecución de pruebas de desarrollo sobre la funcionalidad construida en la iteración.

Una vez construida la aplicación se realizaron las validaciones funcionales y de seguridad que se explican en la siguiente sección.

3.5. Validación de la aplicación

En esta etapa se validó la aplicación desarrollada desde el punto de vista funcional y de seguridad. En la **Figura 9** se muestra el proceso.

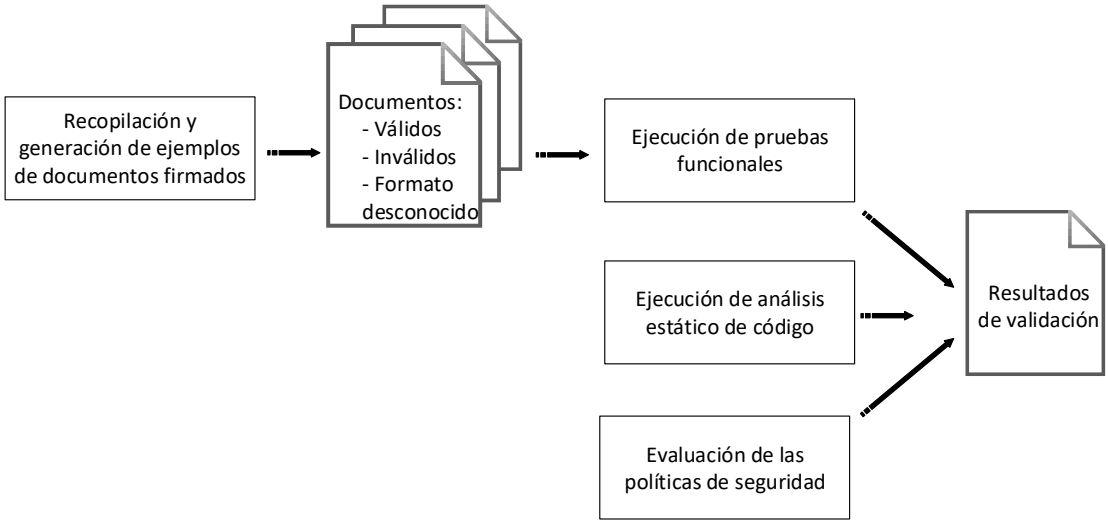

Figura 9. Proceso de validación de la aplicación.

Inicialmente se definieron las pruebas funcionales y para poder ejecutarlas se utilizaron los siguientes documentos:

- Documentos firmados válidos, cuyo formato de firma es igual al perfil seleccionado para el desarrollo de la aplicación.
- Documentos firmados inválidos, cuyo formato de firma es igual al perfil seleccionado para el desarrollo de la aplicación.
- Documentos firmados con un formato diferente al oficial.

Los documentos válidos firmados se obtuvieron de los documentos oficiales sobre firma digital del Gobierno de Costa Rica, los cuales están firmados con base en los estándares oficiales. En el caso de los documentos inválidos, se crearon omitiendo información requerida por el estándar. Por último, los documentos con un formato diferente al oficial, se crearon y se firmaron con un formato no reconocido por la aplicación.

Para validar si la aplicación es segura y confiable se utilizaron tres herramientas de análisis estático de código:

- Security Code Scan
- Puma Scan Pro
- VisualCodeGrepper

Estas herramientas permitieron realizar un análisis más completo de la aplicación, ya que es muy común que los resultados del análisis de seguridad de una aplicación varíen según la herramienta utilizada para validarla. Se usaron estas herramientas porque son recomendadas por la organización *Open Web Application Security Project* (OWASP) para analizar aplicaciones escritas en el mismo lenguaje de programación de la aplicación desarrollada [17]. Esta organización es ampliamente reconocida por sus esfuerzos por mejorar la seguridad en el software a nivel mundial.

También, se utilizó la guía "*Guía de requerimientos técnicos para el aseguramiento de la información de los componentes tecnológicos que utilizan certificados y firma digital en aplicaciones de software dentro del Sistema Nacional de Certificación Digital"* [18], elaborada por Alejandro Mora Castro en su TFIA "*Definición de un proceso de aseguramiento de la información para los componentes tecnológicos que utilizan certificados y firma digital en una aplicación de software dentro del Sistema Nacional de Certificación Digital*" [19], para determinar si la aplicación cumple o no con las políticas de seguridad que ahí se plantean para este tipo de aplicaciones.

En los siguientes capítulos se describen los resultados de este proyecto.

4. Identificación de los perfiles legalmente válidos para la firma digital en el SNCD de Costa Rica

La implementación de firma digital para la autenticación de usuarios y para la firma de documentos electrónicos son dos de los principales casos de uso de una Infraestructura de Llave Pública. Y debido a que existen muchas maneras de firmar digitalmente un conjunto de datos, ya sea para autenticación o para firma de documentos, es fundamental que existan guías y estándares de firma digital para el correcto funcionamiento de una PKI. Estos estándares establecen los requerimientos, tanto de formato como de contenido, que debe cumplir toda firma digital que sea generada dentro de una PKI y son la base para determinar si es válida o no.

Por lo general, en una PKI se utilizan varios estándares dependiendo del tipo de archivo que se desee firmar digitalmente. Cada uno de los estándares define el formato y los campos que debe tener la firma digital para ese tipo en específico y es muy común que contenga campos opcionales que brindan mayor o menor funcionalidad dependiendo de si se incluyen o no. A estos campos opcionales junto con la funcionalidad que proveen se les denomina perfiles de firma digital y también, es fundamental que en una PKI estén definidos los oficiales. De lo contrario, habría muchas maneras de firmar digitalmente un documento con un mismo formato de firma.

En este capítulo se presentan los resultados del proceso realizado para la identificación de los estándares y los perfiles de los formatos de firma digital de documentos legalmente válidos dentro del SNCD de Costa Rica.

4.1. Identificación de los perfiles

La identificación de los perfiles oficiales es uno de los resultados de la primera etapa metodológica. A continuación, se explica qué información contiene cada uno de los documentos oficiales del Gobierno de Costa Rica en relación con los formatos de firma digital.

4.1.1. Ley de certificados, firmas digitales y documentos electrónicos Nº 8454

La Ley Nº 8454 es la base jurídica de la firma digital en Costa Rica [3]. Dicha Ley está redactada de manera que brinda las pautas generales para la firma digital en el país sin dar detalles o requerimientos técnicos que podrían cambiar en un futuro. Esto porque en Costa Rica las modificaciones a las leyes de la República son difíciles de ejecutar. Es por eso que en el Artículo 33, se establece que la Ley será reglamentada posteriormente por el Poder Ejecutivo:

> *ARTÍCULO 33.– Reglamentación*
> *El Poder Ejecutivo reglamentará esta Ley dentro de los seis meses siguientes a su publicación.*

A pesar de que no contienen información sobre los documentos oficiales, algunos de los artículos de la Ley nos dan información sobre las características que deben de tener los estándares y perfiles de documentos firmados digitalmente. Por ejemplo, en el Capítulo II - Documentos, Artículo 6, se menciona que los documentos firmados digitalmente se deben de poder utilizar para referencias futuras, es decir, no deben perder su validez con el tiempo y deben preservar información sobre su origen [3]:

> *ARTÍCULO 6.– Gestión y conservación de documentos electrónicos*
> *Cuando legalmente se requiera que un documento sea conservado para futura referencia, se podrá optar por hacerlo en soporte electrónico, siempre que se apliquen las medidas de seguridad necesarias para garantizar su inalterabilidad, se posibilite su acceso o consulta posterior y se preserve, además, la información relativa a su origen y otras características básicas.*

4.1.2. Reglamento a la ley de certificados, firmas digitales y documentos electrónicos

En el 2006 la DCFD publicó el *Reglamento a la ley de certificados, firmas digitales y documentos electrónicos* [4]. Este reglamento complementa la Ley, incluye disposiciones

detalladas sobre certificados, firmas digitales y documentos electrónicos. Sin embargo, no incluye requerimientos técnicos o estándares sobre los formatos de los documentos firmados digitalmente, sino que al igual que la Ley delega las especificaciones técnicas a políticas que sean emitidas por la DCFD, esto se puede observar en el Artículo 2 donde se define el concepto de lineamientos técnicos [4]:

> *Artículo 2º– Definiciones. Para los efectos del presente Reglamento, se entenderá por:*
> *...30) LINEAMIENTOS TÉCNICOS: El conjunto de definiciones, requisitos y regulaciones de carácter técnico–informático, contenido en la Norma INTE /ISO 21188 versión vigente y en las políticas que al efecto emita la DCFD.*

Además, en el Artículo 24 del reglamento se establece que una de las funciones de la DCFD es la de ser el emisor y gestor de las políticas para el uso de certificados digitales, y como se ha mencionado anteriormente uno de los usos de los certificados digitales es la firma digital de documentos y transacciones electrónicas:

> *Artículo 24.– Funciones. La Dirección de Certificadores de Firma Digital (DCFD) tendrá las funciones que señala la Ley. El registro de certificados digitales a que se refiere el inciso b) del artículo 24 de la Ley tendrá un contenido y propósitos puramente cuantitativos y estadísticos.*
> *La DCFD tendrá la responsabilidad de definir políticas y requerimientos para el uso de certificados digitales que deberán ser especificados en una Política de Certificados o acuerdos complementarios; en especial la DCFD será el emisor y el gestor de las políticas para el Sistema de Certificadores de Firma Digital.*

4.1.3. Política de formatos oficiales de los documentos electrónicos firmados digitalmente

Una de las políticas que ha publicado la DCFD es la *Política de formatos oficiales de los documentos electrónicos firmados digitalmente* (2013) [2]. Esta política define las

características que conforman los formatos oficiales de documentos electrónicos firmados digitalmente, al amparo de la Ley No. 8454 y de su Reglamento, e indica, que estas características deberán ser incorporadas por el firmante, receptor o validador de un documento electrónico en los procesos de generación o validación de firma digital.

En la sección 5 de la política se establece que en el SNCD los formatos oficiales de los documentos electrónicos firmados digitalmente son aquellos construidos con base en los formatos avanzados emitidos como normas técnicas y estándares por la ETSI a partir de la Directiva 1999/93/EC, en un nivel de especificación (perfil) que contemple la inclusión de todos los atributos necesarios para garantizar la verificación de su validez en el tiempo de manera irrefutable. En la **Tabla 3** se presentan los formatos y perfiles que cumplen con dichas características y que se encuentran documentados como oficiales en la política:

Tabla 3. Formatos y perfiles oficiales para la firma digital de documentos dentro del SNCD [2].

Formato	Perfil	Nombre
CAdES: Estándar para firma electrónica avanzada de documentos en formato binario.	**X-L (*eXtended Long*)**: Perfil del estándar CAdES para la garantizar la verificación de la validez de la firma en el tiempo.	**CAdES-X-L**
PAdES: Estándar para firma electrónica avanzada de archivos PDF (*PDF Advanced Electronic Signature*).	**LTV (*Long Term Validation*)**: Perfil del estándar PAdES para la garantizar la verificación de la validez de la firma en el tiempo.	**PAdES LTV** (*Long term validation*)
XAdES: Estándar para firma electrónica avanzada de documentos en formato XML.	**X-L (*eXtended Long*)**: Perfil del estándar XAdES para la garantizar la verificación de la validez de la firma en el tiempo.	**XAdES-X-L**

Estos formatos oficiales deben ser acogidos como el estándar en el cual se basarán los documentos electrónicos firmados digitalmente por toda entidad pública, empresa privada o particular y por lo tanto toda solución de firma digital, interna, interinstitucional o para servicios ofrecidos a clientes, debe ser implementada de acuerdo a los lineamientos de la política [2].

En la siguiente sección se brinda una breve explicación de cada uno de los perfiles.

4.2. Perfiles oficiales de la ETSI

A continuación, se explican los perfiles oficiales de firma digital de documentos electrónicos en Costa Rica.

4.2.1. CAdES-X-L

Se basa en la especificación ETSI TS 101 733 para la firma de documentos con información codificada en binario [13].

El perfil CAdES-X-L es una extensión del perfil CAdES-C. Como se puede observar en la **Figura 10** el perfil CAdES-C incluye las referencias a los certificados y a las listas de revocación (CRLs) o respuestas de OCSP requeridas para la validación de la firma. Por otra parte, el perfil CAdES-X-L incluye la información completa de los certificados y las CRLs o respuestas OCSP no solo las referencias.

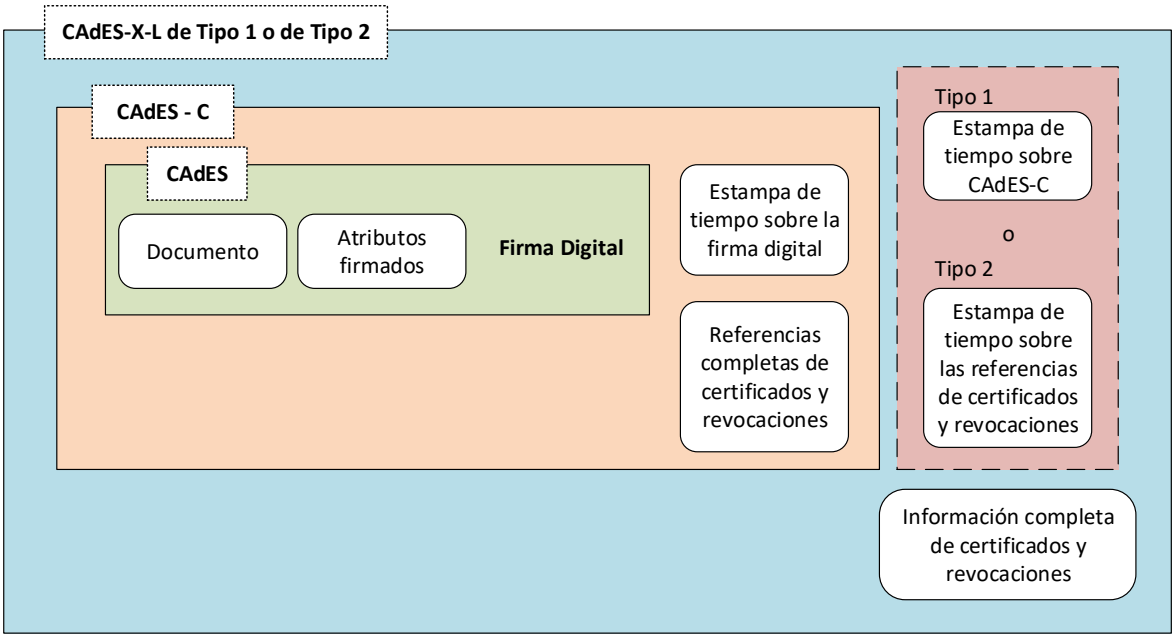

Figura 10. Perfiles del formato CAdES. Tomado de [13].

Este perfil puede ser combinado con los perfiles CAdES-X Type 1 y CAdES-X Type 2 y se le conoce como CAdES-X-L Type 1 or 2. El CAdES-X Type 1 agrega un sello de tiempo para proveer integridad y protección de tiempo sobre todos los elementos y referencias de CAdES-C en caso de que la llave de la CA, CRL o OCSP se vean comprometidos. Y el CAdES-X Type 2 agrega un sello de tiempo solo para las referencias de los certificados y las CRLs o las respuestas OCSP.

4.2.2. PAdES LTV

El perfil PAdES LTV está basado en la especificación ETSI TS 102 778 para la firma de documentos con formato PDF. [15]

Este perfil puede ser utilizado en conjunto con los perfiles PAdES-CMS, PAdES-BES o PAdES-EPES y aplica cuando es necesario validar la firma en un periodo extendido de tiempo, más allá del tiempo de validez del certificado utilizado para la firma.

En la **Figura 11** se presenta la estructura de un documento PDF firmado digitalmente con PAdES-LTV. Al igual que el perfil CAdES-X-L descrito anteriormente, este perfil incluye en el documento firmado la información necesaria para la validación: certificados, CRLs o respuestas OCSP y sellos de tiempo.

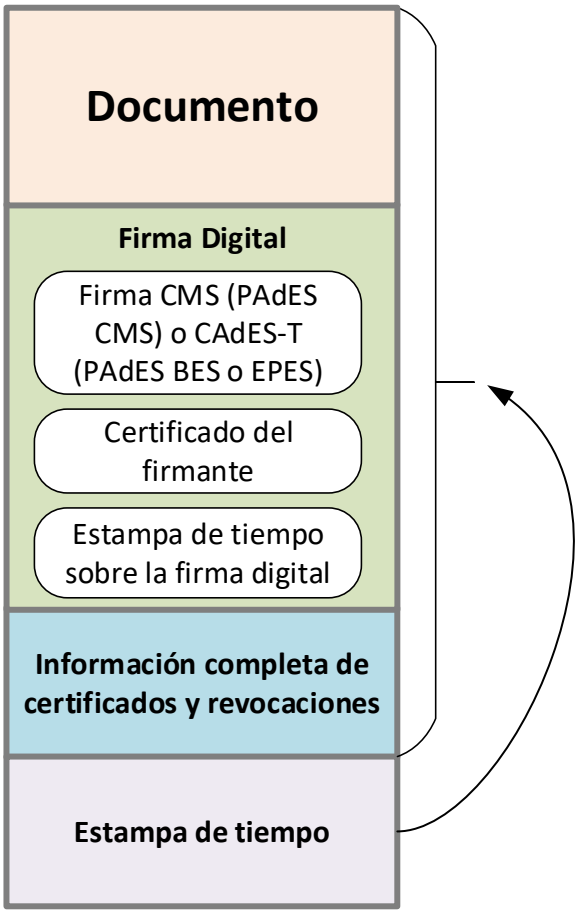

Figura 11. Perfil PAdES LTV. Tomado de [15].

4.2.3. XAdES-X-L

Se basa en la especificación ETSI TS 101 903 para la firma de documentos con formato XML [14].

Se le conoce como *Extended long electronic signatures with time* y es una extensión del perfil XAdES-C. El perfil XAdES-C incluye referencias a la información de validación:

referencias a los certificados y a las listas de revocación (CRLs) o respuestas de OCSP requeridas para la validación de la firma. En el caso del perfil XAdES-X-L, este incluye la información completa de los certificados y las CRLs o respuestas OCSP no solo las referencias.

Este perfil se construye con los perfiles XAdES-X Type 1 y 2. El perfil XAdES-X Type 1 agrega uno o varios sellos de tiempo para proveer integridad y protección de tiempo sobre el elemento de la firma (SignatureValue), el sello o estampa de tiempo de la firma (SignatureTimestamp) y los elementos que contienen las referencias de los certificados y las CRLs o respuestas OCSP (CompleteCertificateRefs y CompleteRevocationRefs). El XAdES-X Type 2 agrega un sello de tiempo solo para las referencias de los certificados y las CRLs o las respuestas OCSP (CompleteCertificateRefs y CompleteRevocationRefs). En la **Figura 12** se puede observar la estructura de XAdES-X-L.

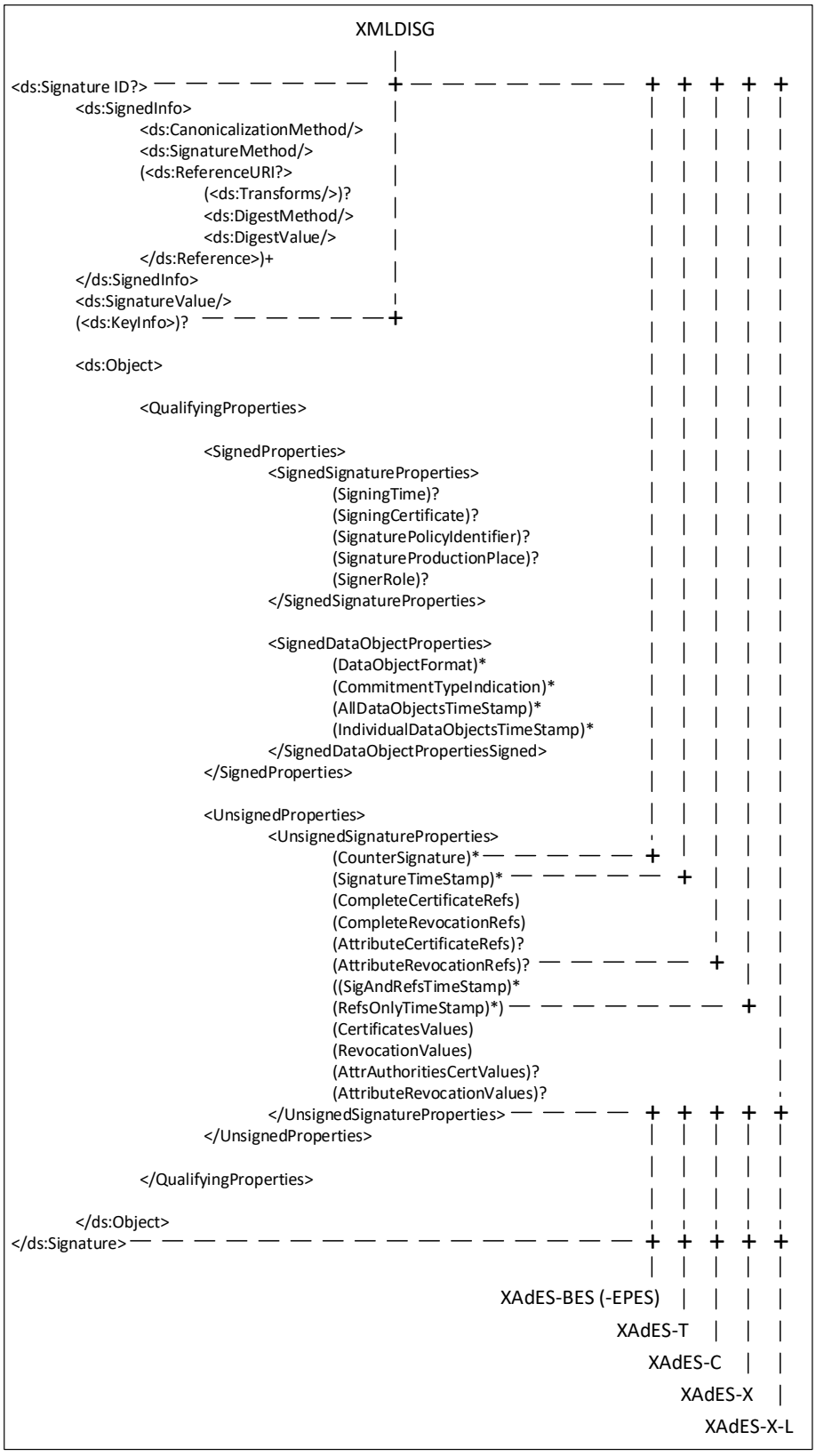

Figura 12. Perfil XAdES-X-L. Tomado de [14].

En la siguiente sección se evalúa si estos perfiles satisfacen las necesidades del país en materia de firma digital.

4.3. Valoración del cumplimiento de los requerimientos de firma digital de los perfiles oficiales dentro el SNCD

En esta sección se presenta una valoración sobre el cumplimiento de los requerimientos de firma digital de documentos de los perfiles oficiales en relación con la regulación del SNCD. Primero, por cada documento oficial que se revisó, se describen los requerimientos que están presentes sobre los perfiles oficiales. Posteriormente, se muestra el control cruzado entre los requerimientos encontrados y las características de los perfiles oficiales, y se describe si cumplen o no con los requerimientos.

4.3.1. Requerimientos de firma digital de la ley de certificados, firmas digitales y documentos electrónicos Nº 8454

En el artículo 6 de la ley se establece que un documento debe poder ser conservado para el futuro y debe de mantener todas sus características para poder validarlo [3]:

> *ARTÍCULO 6.– Gestión y conservación de documentos electrónicos*
>
> *Cuando legalmente se requiera que un documento sea conservado para futura referencia, se podrá optar por hacerlo en soporte electrónico, siempre que se apliquen las medidas de seguridad necesarias para garantizar su inalterabilidad, se posibilite su acceso o consulta posterior y se preserve, además, la información relativa a su origen y otras características básicas.*

En los artículos 8 y 10 se menciona que una firma digital debe permitir verificar la integridad de un documento y debe de identificar de manera unívoca y vincular jurídicamente al autor del documento [3]:

> *ARTÍCULO 8.– Alcance del concepto*
>
> *Entiéndese por firma digital cualquier conjunto de datos adjunto o lógicamente*

asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.

Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.

ARTÍCULO 10.– Presunción de autoría y responsabilidad

Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.

4.3.2. Requerimientos de firma digital de la política de formatos oficiales de los documentos electrónicos firmados digitalmente

En la política de formatos oficiales de los documentos electrónicos firmados digitalmente, se establecen de manera más concreta los requerimientos que deben satisfacer los formatos oficiales [2]:

- Permiten la utilización de algoritmos criptográficos robustos.
- Respetan el principio de neutralidad tecnológica:
    - Son estándares abiertos.
    - Pueden ser empleados en escenarios multiplataforma.
    - No están sujetos a un determinado producto licenciado.
- Están auspiciados por alguna entidad internacional reconocida:
    - Cuentan con una adecuada documentación técnica.
    - Sus especificaciones técnicas sean de acceso público.
- Permiten la incorporación de múltiples firmas en un documento electrónico.
- Implementan los principios de un mecanismo de firma confiable:
    - Garantía de la **autenticidad** del documento electrónico.
    - Garantía de la **integridad** del documento electrónico.
    - Ubicación fehaciente del documento electrónico en el **tiempo**.

- Especifican mecanismos estandarizados para garantizar la preservación y verificación de la validez de las firmas digitales del documento electrónico en el tiempo:
    - Inclusión de **sellos de tiempo** en el documento.
    - Inclusión de la **ruta de certificación** en el documento.
    - Inclusión de la **información de revocación** en el documento.

A continuación, se valora cada uno de estos requerimientos con respecto a las características de los formatos oficiales de la ETSI:

4.3.2.1. Permiten la utilización de algoritmos criptográficos robustos

Los tres estándares de formato de firma avanzada (AdES): XAdES, CAdES y PAdES cumplen con este requerimiento. Los estándares permiten que cualquier algoritmo criptográfico robusto pueda ser utilizado siempre y cuando sea confiable. Una característica importante de ellos es que no establecen de forma específica los algoritmos criptográficos que se deben de usar para generar el resumen o la firma, ya que estos pueden ser vulnerados en cualquier momento.

Sin embargo, en el estándar ETSI TS 102 176-1 [20] se hacen recomendaciones de funciones *hash* y de algoritmos asimétricos que se pueden usar con los formatos para la firma digital de documentos. Por ejemplo, en la **Tabla 4** se presentan las suites de firma recomendadas. Una *suite* de firma está compuesta de una función *hash*, un método de *padding* y un algoritmo de firma:

Tabla 4. Recomendaciones de algoritmos criptográficos por la ETSI.

Nombre de la *suite* de firma	Función *hash*	Método *padding*	Algoritmo de firma
sha256-with-rsa	sha256		rsa
rsa-pss with mgf1SHA256Identifier	mgf1SHA-256	No aplica	rsa
sha256-with-ecdsa	sha256	No aplica	ecdsa-Fp o ecdsa-F2m
sha384-with-ecdsa	sha384	No aplica	ecdsa-Fp o ecdsa-F2m
sha512-with-ecdsa	sha512	No aplica	ecdsa-Fp o ecdsa-F2m

4.3.2.2. Respetan el principio de neutralidad tecnológica

Los estándares AdES de la ETSI también cumplen con este requisito. Son estándares abiertos que están disponibles al público sin ningún costo y cualquier entidad que desee implementarlos puede hacerlo. También, son estándares que pueden implementarse en cualquier plataforma, no están limitados a un sistema operativo o dispositivo. De hecho, los tres estándares solo hacen referencia a tipos de archivos (XML, PDF y binario), los cuales pueden ser manejados en cualquier sistema operativo con el software correspondiente.

4.3.2.3. Están auspiciados por alguna entidad internacional reconocida

Efectivamente, los estándares oficiales cumplen con este requerimiento. Todos han sido desarrollados por la ETSI, que es una organización de estándares europeos, reconocida como tal por la Unión Europea. Esta entidad provee estándares en las tecnologías de la información y la comunicación a nivel mundial. Todos estos estándares cuentan con documentación técnica clara y de acceso público. Por ejemplo:

- ETSI TS 102 176-1 [20]
- ETSI TS 101 733 [13]
- ETSI TS 102 778 [15]
- ETSI TS 101 903 [14]

4.3.2.4. Permiten la incorporación de múltiples firmas en un documento electrónico

Los tres estándares permiten la incorporación de múltiples firmas en un mismo documento, aunque de diferente manera.

Los formatos CAdES y XAdES tienen dos tipos o categorías de firmas múltiples:

- Firmas independientes: Son firmas paralelas en donde el orden de las firmas no es importante. Se pueden tener múltiples firmas sobre la misma información.
- Firmas incrustadas (*embedded)*: Son firmas aplicadas una después de la otra, en donde el orden de las firmas si es importante. Existe la capacidad de firmar datos previamente firmados.

En el caso del formato PAdES solamente se pueden agregar firmas múltiples en serie, siguiendo un orden, donde la firma actual firma los datos previamente firmados. En la **Figura 13** se muestra la estructura de múltiples firmas en el formato PAdES:

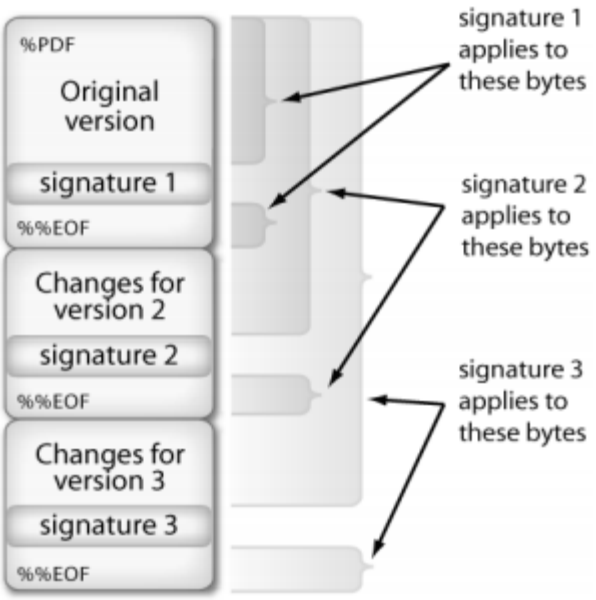

Figura 13. Múltiples firmas en el formato PAdES. Tomado de [15].

4.3.2.5. Implementan los principios de un mecanismo de firma confiable

Todos los estándares AdES proveen los servicios de autenticidad e integridad, y permiten la ubicación fehaciente del documento electrónico en el tiempo, por lo que si cumplen con este requerimiento.

Para proveer autenticidad incluyen dentro de la firma electrónica el certificado de la persona que firma el documento y se basan en los mecanismos de seguridad de una PKI para lograrlo. Por ejemplo, establecen el uso de OCSP para la solicitud y verificación de certificados. En el caso de integridad, todos requieren del uso de una función hash robusta que permita generar un resumen del documento para incorporarlo a la firma y posteriormente utilizarlo para verificar si no ha ocurrido algún cambio en el documento.

Por último, todos los estándares AdES definen campos o atributos para incluir sellos de tiempo que permiten garantizar la validez de una parte o de todos los datos incluidos en la firma.

4.3.2.6. Especifican mecanismos estandarizados para garantizar la preservación y verificación de la validez de las firmas digitales del documento electrónico en el tiempo

Los tres perfiles oficiales, XAdES-XL, CAdES-XL y PAdES LTV establecen la necesidad de incluir sellos de tiempo para garantizar la validez de la información en el tiempo, de manera que efectivamente cumplen con el presente requisito.

También, definen campos requeridos para agregar las listas de certificados y las listas de revocación o respuestas de OCSP, las cuales permiten que las firmas digitales generadas con dichos estándares y los documentos prevalezcan en el tiempo.

En la **Tabla 5** se presenta un resumen de la valoración presentada en esta sección.

Tabla 5. Resumen de la valoración del cumplimiento de los perfiles en el SNCD.

Origen del requerimiento	Requerimiento	Cumplen		Observaciones
		Si	No	
Artículo 6 de la Ley Nº 8454	Un documento debe poder ser conservado para el futuro y debe de mantener todas sus características para poder validarlo	X		Los tres estándares incorporan en la firma la información necesaria para que los documentos prevalezcan en el tiempo: la lista de certificados, CRLs, sellos de tiempo, entre otros.
Artículo 8 de la Ley Nº 8454	Una firma digital debe permitir verificar la integridad de un documento	X		Los estándares permiten utilizar funciones hash robustas para calcular el resumen del documento original que se incorpora en la firma, para posteriormente validar la integridad del documento.
Artículo 10 de la Ley Nº 8454	Una firma digital debe permitir identificar de manera unívoca y vincular jurídicamente al autor del documento	X		En todos los estándares la firma se calcula con la llave privada del firmante y se incluye en ella su certificado, el cual incluye la llave publica que se utilizará para validar que el documento efectivamente fue firmado por el autor.
Política de formatos oficiales	Permiten la utilización de algoritmos criptográficos robustos	X		Los tres estándares de formato de firma avanzada (AdES): XAdES, CAdES y PAdES permiten utilizar algoritmos criptográficos robustos. No establecen los algoritmos que se deben usar, ya que en cualquier momento pueden ser vulnerados.

Origen del requerimiento	Requerimiento	Cumplen		Observaciones
		Si	No	
Política de formatos oficiales	Respetan el principio de neutralidad tecnológica	X		Los estándares AdES de la ETSI son estándares abiertos que están disponibles al público sin ningún costo y cualquier entidad que desee implementarlos puede hacerlo.
Política de formatos oficiales	Están auspiciados por alguna entidad internacional reconocida	X		Están auspiciados por la ETSI, que es una organización de estándares europeos reconocida por la Unión Europea.
Política de formatos oficiales	Permiten la incorporación de múltiples firmas en un documento electrónico	X		Todos los estándares lo permiten. CAdES y XAdES permiten agregar múltiples firmas independientes o incrustadas. Y PAdES permite agregarlas en serie.
Política de formatos oficiales	Implementan los principios de un mecanismo de firma confiable	X		Los estándares oficiales permiten garantizar la autenticidad, integridad y ubicación en el tiempo del documento. Por medio de mecanismos como la inclusión del certificado del firmante en la firma, la utilización de funciones hash robustas y la estampa de tiempo, respectivamente.
Política de formatos oficiales	Especifican mecanismos estandarizados para garantizar la preservación y verificación de la validez de las firmas digitales del documento electrónico en el tiempo	X		Los tres estándares incorporan en la firma la lista de certificados, CRLs y sellos de tiempo, que permiten que los documentos prevalezcan en el tiempo.

4.4. Análisis de los formatos y selección de al menos uno para ser validado por la aplicación

En esta sección se describen los resultados de la caracterización de los perfiles oficiales y el uso de estas características como criterios de selección del formato que debe validar la aplicación. Primero, se presentan las características más relevantes de cada estándar, luego el formato seleccionado y, por último, las razones de su elección.

En la **Tabla 6** se presentan las características más importantes que se obtuvieron durante el análisis de los formatos oficiales. En el Apéndice A. Características de los formatos oficiales de firma digital dentro del SNCD., se encuentra la tabla completa.

Tabla 6. Características extraídas de los formatos oficiales.

Formato	Tipo de archivo	Otros formatos requeridos	Nivel de complejidad de desarrollo	Aplicación disponible para su validación	Existe guía de desarrollo oficial	Utilidad
XADES	XML	CADES	Media	Si	Si	Alta
CADES	Binario	-	Media	No	No	Media
PADES	PDF	CADES	Alta	No	No	Alta

Con base en las características obtenidas se descartó el formato XAdES, ya que, a pesar de que es un formato muy útil por la interoperabilidad que proporciona el tipo de archivo XML, el BCCR como ente encargado de soportar la plataforma tecnológica del país en el tema de firma digital, cuenta con herramientas desarrolladas por ellos mismos para la firma y validación de este tipo de firmas digitales. Incluso tienen disponible una guía de desarrollo en el momento de realizar la investigación. Por lo tanto, el aporte que podría brindar este trabajo al proyecto en el cual se desarrolla se vería reducido.

Posteriormente, se procedió a analizar los formatos restantes CAdES y PAdES. En ambos casos, el BCCR no cuenta con herramientas desarrolladas para la firma y validación del formato, ni con una guía de desarrollo, solamente proporciona guías de uso de herramientas de terceros. En el caso de CAdES tiene a disposición la guía “Guía de Firma Digital para

XólidoSign" [21], en la cual se recomienda cómo utilizar y configurar la herramienta XólidoSign para la firma y validación en formato CAdES-XL. Para PAdES existen las siguientes guías:

- "Guía de Firma Digital para Adobe Reader XI" [22]
- "Guía de Firma Digital para Adobe Reader XI en Mac" [23]
- "Guía de Firma Digital para Adobe Reader DC" [24]

En estas guías se recomienda como utilizar la herramienta Adobe Reader XI en sistemas operativos Windows, Adobe Reader XI en sistemas operativos Mac y Adobe Reader DC, respectivamente, para la firma y validación de este tipo de firma. Esta situación limita a aquellas personas o entidades públicas o privadas que desean realizar sus propios desarrollos a usar herramientas de terceros, las cuales podrían no ser integrables con sus aplicaciones. Por lo tanto, es importante poder contar con una aplicación de ejemplo que valide estos formatos y que pueda ser utilizada por estas personas o entidades para sus propios desarrollos.

A pesar de que en ambos casos se presenta esta necesidad, para este proyecto se seleccionó solamente el formato PAdES LTV para el desarrollo de la aplicación, por las siguientes razones:

- Primero, porque el tipo de archivo PDF es ampliamente utilizado en el país para compartir documentos, por encima del formato binario. Por ejemplo, es poco común compartir documentos en imágenes y tener la necesidad de firmarlas en formato binario, sin embargo, si se presentara este caso de uso se cuenta con la posibilidad de utilizar XML con el formato de firma XAdES-XL y alguna de las aplicaciones que ya tiene disponible el BCCR para este perfil.
- Segundo, aunque la aplicación desarrollada sea para validar el perfil de firma PAdES LTV, también incluirá la lógica para manejar y validar el formato CAdES básico, ya que como se muestra en la **Tabla 6** este formato es requerido en el formato PAdES. Esto quiere decir que con esta aplicación se estaría realizando un aporte significativo, brindando un ejemplo sobre cómo manejar y validar archivos firmados con PAdES LTV y sentando las bases para validar el formato CAdES-XL.

- Tercero, el tiempo disponible para el desarrollo de la aplicación es limitado. Lo ideal sería poder contar con el tiempo necesario para desarrollar una aplicación de ejemplo que permita validar los dos formatos restantes o incluso los tres para contar con una sola base. Sin embargo, esto no es posible por el tiempo disponible para finalizar este proyecto. Por lo tanto, se ha seleccionado un formato que brinda un aporte significativo, tiene un nivel de complejidad adecuado y el cual es posible desarrollarlo en el tiempo que se tiene disponible.

En el siguiente capítulo se presenta una descripción de la aplicación desarrollada para la validación del formato seleccionado (PAdES LTV) y de los componentes que la conforman.

5. Desarrollo de una aplicación de software para la validación de los formatos oficiales de firma digital dentro del SNCD de Costa Rica

En este capítulo se describe la aplicación desarrollada. Primero, se muestran los estándares que contienen los requerimientos de la aplicación, luego se brinda una descripción general de la aplicación, posteriormente se detallan cada uno de sus componentes y, por último, se explican las herramientas de terceros que se utilizaron para su desarrollo.

5.1. Requerimientos de la aplicación

Los requerimientos de la aplicación se obtuvieron directamente de los estándares de la ETSI y de la ISO. En la **Tabla 7** se muestran los estándares consultados y se brinda una explicación sobre los requerimientos que contiene cada uno de ellos.

En la siguiente sección se describe la aplicación desarrollada con base en estos requerimientos.

Tabla 7. Estándares internacionales consultados para requerimientos de la aplicación.

Estándar	Detalle
ISO 32000-1: Document management - Portable document format - Part 1: PDF 1.7 [25]	Este estándar especifica el tipo de archivo PDF. Contiene los requerimientos para la correcta manipulación de contenido y firma digital de documentos PDF, entre otros.
ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES) [13]	Contiene la especificación de firmas digitales en formato CAdES. Se consultó porque el formato PAdES requiere que una parte de la firma en el archivo PDF sea calculada siguiendo este formato.
ETSI TS 102 176-1: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms [20]	Especifica cuales son los algoritmos y funciones hash recomendados para la firma y validación de documentos firmados.
ETSI EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation [26]	Contiene los requerimientos de una aplicación que firme y/o valide los formatos AdES. De este estándar se obtuvieron los requerimientos arquitectónicos y de flujo de información de la aplicación.
ETSI TS 102 778-1: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES [15]	Este estándar contiene la especificación del formato de firma PAdES, así como una explicación general de los diferentes perfiles de este formato y sus relaciones.
ETSI TS 102 778-2: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1 [27]	Es la especificación del perfil básico PAdES, el cual se basa en el estándar ISO 32000-1 de firma digital de archivos PDF. Este contiene los requerimientos base de cualquier firma PAdES sin importar el perfil.

Estándar	Detalle
ETSI TS 102 778-3: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles [28]	Este estándar contiene los requerimientos de una firma PAdES en sus perfiles PAdES-BES y PAdES-EPES. Los elementos que incluyen estos perfiles a la firma, son requeridos por el perfil PAdES LTV, por lo que son parte de los requerimientos de la aplicación.
ETSI TS 102 778-4: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile [29]	Contiene la especificación del perfil PAdES LTV. Todos los elementos que corresponden únicamente a este perfil se detallan en este estándar. Es necesario para la correcta manipulación de los elementos LTV.

5.2. Descripción de la aplicación

La aplicación desarrollada se denomina “Validador de formato de firma PAdES LTV” y como su nombre lo indica permite validar firmas digitales avanzadas de archivos PDF en formato PAdES LTV. Sin embargo, está diseñada de manera que en un futuro se pueda agregar soporte de validación de los otros formatos de firma avanzada oficiales en el SNCD (XAdES X-L y CAdES X-L).

Es una aplicación de tipo consola, escrita en el lenguaje de programación C# del *framework* de desarrollo .NET de Microsoft. La decisión de desarrollarla en este lenguaje se tomó en forma conjunta con expertos del BCCR y el MICITT, ya que la mayoría de herramientas de firma digital que se han desarrollado al momento de la investigación están escritas en este lenguaje y es apropiado continuar en la misma línea de desarrollo.

La arquitectura de la aplicación está basada en el modelo de validación de firma del estándar de la ETSI EN 319 102-1 [26] (ver **Figura 14)**. Por lo que se divide en dos grandes componentes, el componente de validación de firma y el componente de conducción.

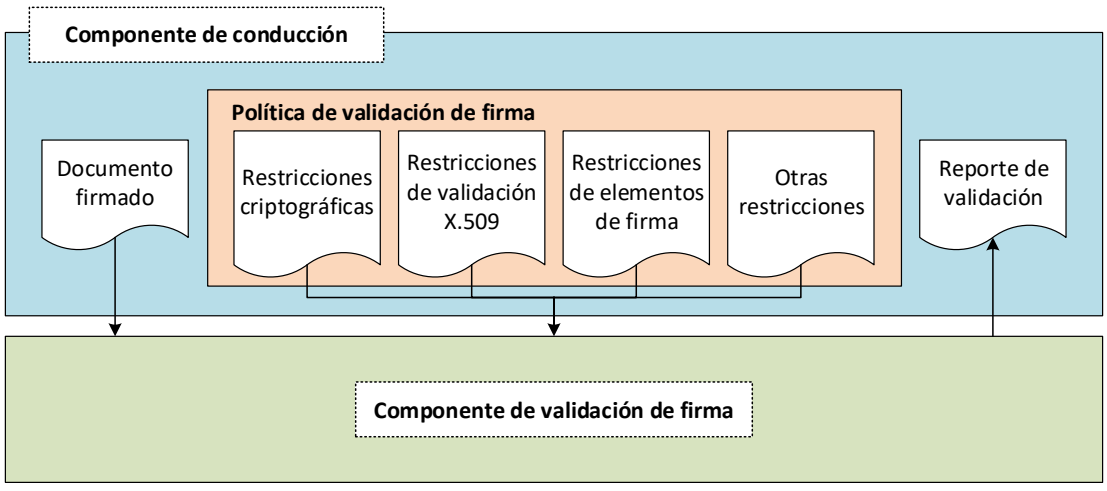

Figura 14. Modelo conceptual de la aplicación

El componente de conducción se encarga de proveerle al componente de validación todos los insumos necesarios para validar la firma. Estos insumos son el documento firmado y la

configuración necesaria para validar la firma. La política de validación de firma es parte de esa configuración, la cual consiste en un archivo XML que contiene un conjunto de restricciones de validación que pueden variar según los requerimientos de firma digital de la PKI en donde se utilice. Puede incluir, por ejemplo, los algoritmos criptográficos válidos dentro de la PKI para la firma digital, restricciones de certificados, restricciones de la estampa de tiempo, entre otras. En el Apéndice B. Política de validación de firma de la aplicación, se presenta la política de validación utilizada en este proyecto.

El componente de validación de firma contiene los elementos requeridos para la validación de una firma PAdES LTV. La validación la realiza basándose en las restricciones de la política de validación y retorna como resultado tres elementos, un reporte detallado, un reporte simple y datos de diagnóstico. Estos se describen en la **Tabla 8** y en el Apéndice C. Ejemplos de resultados de la aplicación, se muestra un ejemplo de cada uno de ellos.

Tabla 8. Resultados de validación de firma de la aplicación.

Resultado	Descripción
Reporte detallado *o Detailed Report*	Información detallada sobre el resultado de la validación de la firma, basada en el estándar ETSI EN 319 102-1 [26].
Reporte simple *o Simple Report*	Información resumida sobre el resultado de validación de la firma y un indicador del estado de la firma. Se obtiene del reporte detallado.
Datos de diagnóstico *o Diagnostic Data*	Información sobre la firma digital que se está validando y sobre información obtenida durante la validación.

El reporte detallado incluye un indicador de estado para cada restricción de validación.

En la **Tabla 9** se presentan los posibles indicadores de estado para cada restricción de validación y su significado.

Tabla 9. Posibles estados de una restricción de validación.

Estado	Significado
PASSED	Todas las verificaciones correspondientes al bloque de validación pasaron.
INDETERMINATE	La información disponible sobre la firma es insuficiente para ejecutar todas las verificaciones correspondientes al bloque.
FAILED	Si el estado no es *PASSED* o *INDETERMINATE*

El reporte simple también incluye un indicador de estado y detalles adicionales sobre la validación completa de la firma. En la **Tabla 10** se muestran los posibles indicadores.

Tabla 10. Posibles estados de la validación completa de una firma.

Estado	Significado	Información adicional
TOTAL-PASSED	Todas las verificaciones pasaron.	• Identidad del firmante • Certificado de firma y cadena de certificados.
TOTAL-FAILED	Si se cumple alguna de las siguientes condiciones: • Las verificaciones criptográficas de la firma fallaron. • Si se prueba que la generación de la firma fue después de la revocación del certificado usado para firmar. • Todas las verificaciones fallaron.	• Explicación adicional sobre la invalidez de la firma. • Las restricciones que generaron el resultado negativo.
INDETERMINATE	La información es insuficiente como para determinar si la validación total es *TOTAL-PASSED* o *TOTAL-FAILED*. Es decir, si falló al menos una verificación que no sea criptográfica y que a su vez no se haya probado que la firma se generó después de la revocación del certificado.	• Explicación adicional sobre el estado de la firma para ayudar al verificador de la firma. • Las restricciones que generaron el resultado.

Por lo tanto, si la aplicación retorna el indicador *TOTAL-PASSED* para un documento firmado, la firma es considerada técnicamente válida. Cualquier otro indicador indica que la firma es inválida.

La aplicación no requiere de una base de datos para almacenar la configuración o la política de validación. Esta información la obtiene de archivos en formato XML. Lo mismo ocurre con los reportes de resultados, estos se almacenan en formato XML en el disco duro, no se necesita una base de datos. También, es importante destacar que la información que se extrae de un documento firmado digitalmente, solamente es almacenada en memoria mientras se está realizando la validación y una vez completado el proceso es eliminada. La única información que se guarda es la que contienen los reportes de resultados y de diagnóstico.

Un resumen de las características más importantes de la aplicación se presenta en la **Tabla 11**.

Tabla 11. Características de la aplicación

Característica	Detalle
Lenguaje de programación	C# de Microsoft .NET
Tipo de aplicación	• Aplicación de consola (el componente de conducción) • Librería de clases (el componente de validación de firma)
Modular	La aplicación está construida de manera modular y cada componente se encarga de tareas específicas.
Flexible	El componente de validación de firma al ser una librería de clases puede ser utilizada en diferentes topologías: • Una aplicación de escritorio • Una aplicación cliente-servidor • Combinación
Extensible	La aplicación al estar desarrollada de manera modular permite agregar nueva funcionalidad fácilmente. En un futuro es posible agregar soporte para validar los otros formatos de firma avanzada.
Reusable	Los componentes de la aplicación se pueden utilizar para soportar los otros formatos de firma digital o incluso para agregar soporte para firmar documentos.
Fiable	El software ha sido altamente probado con diferentes ejemplos de firma y no presenta errores. De igual manera las herramientas de terceros usadas, son ampliamente utilizadas y tienen soporte continuo.
Segura	La aplicación está diseñada siguiendo altos estándares de seguridad.
Diseñada con base en estándares	Su diseño está basado en diferentes estándares internacionales: • Para su arquitectura y procedimientos de validación el estándar ETSI EN 319 102-1. • Para la validación del formato de firma PAdES LTV los estándares ETSI TS 102 778-1 y ETSI TS 102 778-4. • ISO 32000-1 para la manipulación de los documentos PDF. • Y otros en los que se basan los estándares anteriores.

En la siguiente sección se explican los componentes que conforman la aplicación.

5.3. Componentes

En esta sección se describen cada uno de los componentes de la aplicación “Validador de formato de firma PAdES LTV”.

La aplicación está compuesta por 9 componentes en total, los cuales se describen a continuación:

- **Componente de interacción con el usuario o de conducción:** Es el componente encargado de solicitar la ruta del documento firmado digitalmente que se desea validar, proveer la política de validación al componente de validación y presentar los resultados de la validación.
- **Validador de formato del documento:** Este componente verifica que el formato de la firma cumpla con el estándar del formato PAdES. Las validaciones específicas del perfil PAdES-LTV se realizan en el componente “Validador de aceptación de firma”.
- **Identificador del certificado de firma:** Componente responsable de identificar y extraer el certificado de firma que se utilizará para validar la firma.
- **Inicializador del contexto de validación:** Este componente inicializa todas las restricciones incluidas en la política de validación (criptográficas, de elementos de firma, entre otras), así como cualquier otra configuración que provee el componente de conducción (orígenes de datos para la consulta de certificados, para llamadas OCSP, entre otras).
- **Verificador de la información de revocación:** Verifica que la información de revocación sea “fresca” en un momento dado de validación.
- **Validador de X.509:** Valida el certificado de firma, construye y valida la cadena de certificados, verifica el estado de revocación de cada certificado y valida la estampa de tiempo de la firma.

- **Verificador criptográfico:** Este componente valida la integridad del documento firmado, por medio de verificaciones criptográficas.
- **Validador de aceptación de firma:** Realiza verificaciones adicionales, propias del perfil PAdES LTV. Por ejemplo, verificación de otras estampas de tiempo.
- **Componente de reporte de resultados:** Este componente se encarga de general los tres resultados del proceso de validación de firma:
    - El reporte detallado
    - El reporte simple
    - Y la información de diagnóstico

Una descripción de las entradas y salidas de cada componente se muestra en el Apéndice D. Componentes de la aplicación.

5.4. Diagrama de flujo de información de la aplicación

El diagrama de flujo de información que se presenta en esta sección describe el proceso de validación de firma digital de la aplicación desarrollada.

Al igual que la arquitectura de la aplicación, el proceso de validación está completamente basado en el estándar ETSI EN 319 102-1 [26]. Este proceso es guiado por una política de validación y permite la validación de firma PAdES LTV. Además, no solo verifica el formato y la existencia de cierta información, sino que también valida las dependencias de tiempo entre los elementos.

La **Figura 15** muestra el diagrama de flujo. Los componentes descritos en la sección anterior son las bases de construcción del diagrama y en este se presenta la relación entre cada uno de ellos. A continuación, se describe el proceso en una serie de pasos:

1. El flujo comienza cuando el *componente de conducción* recibe un documento firmado para validarlo [1].
2. Posteriormente, este componente provee una serie de configuraciones, la política de validación y el documento firmado al *componente de validación* de firma.
3. Luego, el formato del documento es verificado por el *validador de formato*, si el resultado es *PASSED* el proceso de validación continua con el siguiente paso, que es la identificación del certificado de firma. En caso de que se genere un error durante la validación del formato, retorna *INDETERMINATE* junto con información adicional al error.
4. El *identificador de certificado* recibe el documento firmado y trata de extraer el certificado utilizado para realizar la firma. Si logra extraerlo continúa el proceso, sino retorna *INDETERMINATE* y la razón de no haber podido extraer el certificado.
5. Después, el *inicializador del contexto de validación* inicializa las restricciones criptográficas, X.509 y de elementos de la firma.
6. En el siguiente paso, el *verificador criptográfico* realiza la validación de las restricciones criptográficas de la firma y verifica la integridad del documento. Si el resultado es positivo (*PASSED*) continua con el paso siguiente, sino retorna *INDETERMINATE* o *FAILED* según sea el caso.
7. A continuación, se realizan las validaciones X.509 en el *validador de X.509* a partir del certificado obtenido en el paso 4 y las restricciones incluidas en la política. También, se verifica que tan "fresca" es la información de revocación. Este proceso puede retornar *PASSED* si todas las verificaciones son positivas o *INDETERMINATE*, en cualquier caso, el proceso continúa.
8. Luego, el *validador de aceptación de firma* ejecuta la validación de los elementos de firma LTV, es decir, los elementos de estampa de tiempo adicionales y cualquier otra validación de restricción de los elementos de firma. Por ejemplo, si retorna *PASSED*, pero según la política se debe verificar que el algoritmo de firma sea considerado confiable al momento de la firma (estampa de tiempo de la firma) y éste no lo era, entonces retorna *FAILED.*

[1] El documento debe de haber sido analizado previamente por un antivirus para determinar si incluye algún tipo de virus o código malicioso.

9. Finalmente, el *componente de reporte de resultados* genera los tres reportes (simple, detallado y de diagnóstico) con base en los resultados de cada componente y se los retorna al componente de conducción.

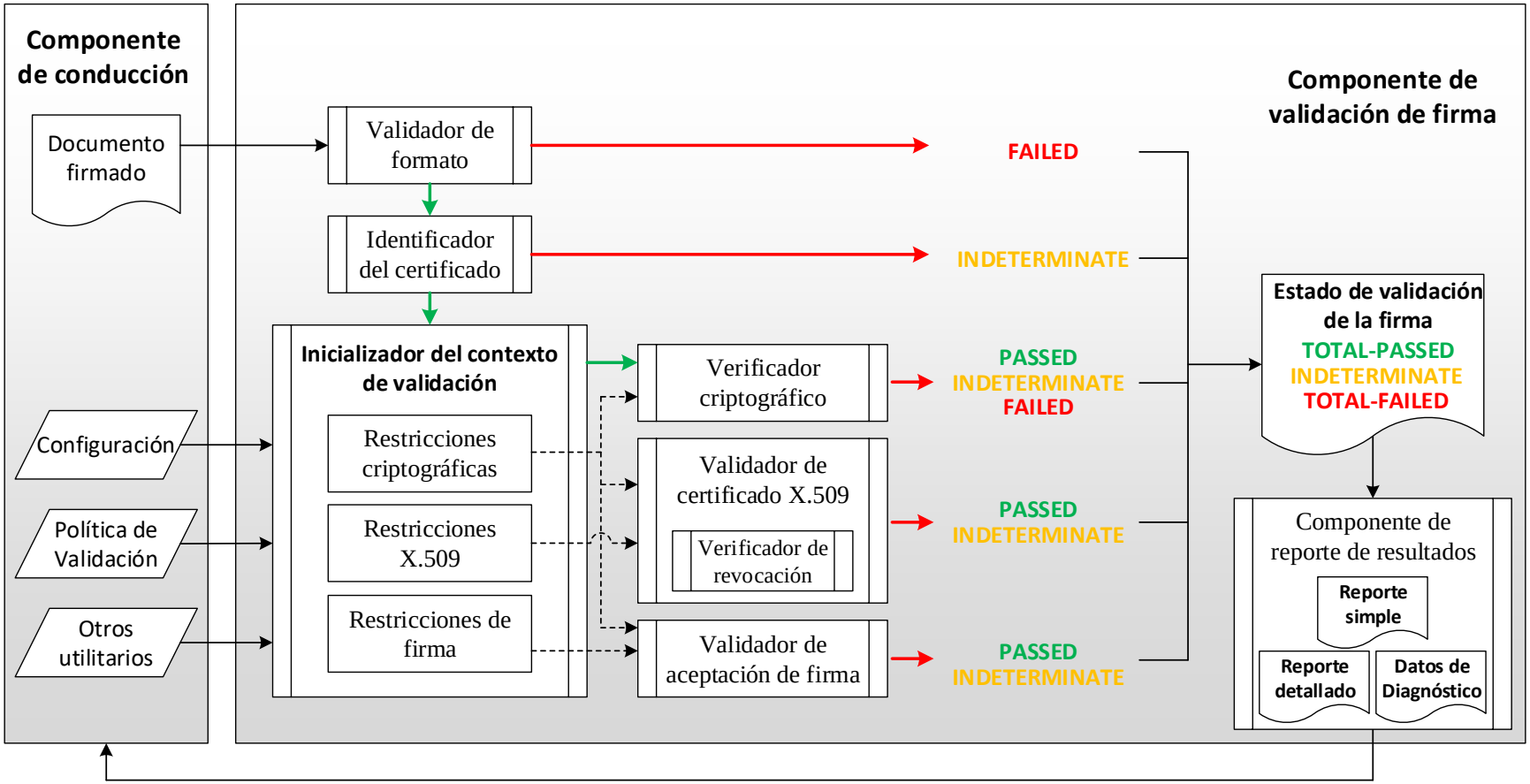

Figura 15. Diagrama de flujo de información del proceso de validación de firma de la aplicación.

5.5. Librerías de terceros utilizadas en la aplicación

Para el desarrollo de la aplicación se utilizaron librerías de terceros que permiten realizar tareas especializadas durante el proceso de validación de la firma. A continuación, se describe la funcionalidad que incluye cada una de ellas.

5.5.1. BouncyCastle C#

BouncyCastle C# es una librería de código abierto especializada en operaciones criptográficas y en manipulación de certificados X.509, CRLs, OCSP, time stamps, entre otras [30]. Se utiliza ampliamente en la aplicación en diversos componentes. Por ejemplo, se usa para extraer y contener la información de certificados X.509, para la generación de *hash* o resumen del documento firmado, para validaciones criptográficas, de CRLs, entre otras.

Esta librería fue escogida para usarla en la aplicación por las siguientes razones:

- Experiencia de sus creadores en criptografía. Su versión en Java tiene 19 años de existir y la versión en C# tiene poco más de 12 años.
- Completa, contiene todas las operaciones requeridas por la aplicación.
- Muy fiable. Es una librería altamente probada y cuyo mantenimiento es continuo.
- Amplia documentación disponible en la web.
- Es muy utilizada, por lo que es fácil encontrar ejemplos sobre cómo implementarla.
- Fácil de usar.

5.5.2. iTextSharp

La librería iTextSharp es una librería de código abierto para la manipulación de archivos PDF [31]. Esta librería se utiliza específicamente para manipular el documento firmado y extraer la firma digital durante la validación del formato.

Algunas de las razones de su uso son:

- Esta desarrollada conforme a estándares, específicamente el PDF 32000-1, requerido por el estándar de la ETSI PAdES para manipular archivos PDF.
- Por su fiabilidad. Su mantenimiento es continuo y es altamente probada.
- Es utilizada por empresas reconocidas como Dell, SIEMENS, entre otras.
- Su sitio web cuenta con muy buena documentación y ejemplos de uso.

5.5.3. Digital Signature Service

DSS es una librería de código abierto escrita en el lenguaje de programación Java, que permite firmar y validar todos los formatos AdES de la ETSI. Fue desarrollada por la Unión Europea y es distribuida por el programa Connecting Europe Facility Digital (CEF Digital).

De esta librería se extrajo la funcionalidad relacionada con la validación de firma del formato PAdES y se migró al lenguaje de programación de la aplicación (C# del *framework* .NET de Microsoft), para utilizarla en la aplicación desarrollada.

Esta librería se utilizó en el presente proyecto de investigación para el desarrollo de la aplicación por las siguientes razones:

- Soporta los estándares europeos de la ETSI, considerados oficiales dentro del SNCD.
- Está desarrollada con base en los estándares de la ETSI.
- Permite asegurar que las firmas son creadas y verificadas de acuerdo con los estándares de la ETSI.
- Es desarrollada por la Unión Europea, organización que reconoce a la ETSI como una organización de estándares para soportar las regulaciones europeas.
- Puede ser reutilizada en cualquier implementación de firma digital.

6. Validación de la aplicación

En este capítulo se presentan los resultados de las validaciones funcionales y de seguridad de la aplicación.

6.1. Validaciones funcionales de la aplicación

Para la validación funcional de la aplicación se definieron los tres escenarios de prueba que se presentan en la **Tabla 12**. Con el primer escenario se desea validar si la aplicación logra identificar correctamente documentos considerados como válidos en el SNCD. El segundo escenario permite validar si la aplicación identifica documentos firmados inválidos, es decir, que no cumplen con la política de validación de firma. Como se mencionó anteriormente, en esta política se establecen las diferentes restricciones de la PKI. Con el tercer escenario se desea validar si la aplicación identifica correctamente aquellos documentos que están firmados con un formato que no es el oficial.

Tabla 12. Escenarios de prueba funcionales.

Id	Nombre	Descripción
1	Identificación de documentos válidos	La aplicación debe identificar documentos PDF considerados válidos dentro del SNCD.
2	Identificación de documentos inválidos	La aplicación debe identificar documentos PDF que presenten algún problema criptográfico, de integridad o que no cumplan con la política de validación.
3	Identificación de documentos con un formato desconocido	La aplicación debe identificar como inválidos los documentos que hayan sido firmados con un formato diferente a PAdES

Para poder ejecutar el escenario 1 se obtuvieron documentos firmados de los documentos oficiales sobre firma digital del Gobierno de Costa Rica, los cuales están firmados con base en los estándares oficiales. También, se crearon y firmaron documentos válidos con base en las guías disponibles en el SNCD. Posteriormente, se modificó la política de validación para

reflejar en ella las restricciones de validación del SNCD. Se configuraron los algoritmos de *hash* y firma válidos, los usos de certificado de firma válidos, la cadena de certificados de confianza y el perfil oficial PAdES LTV. Por último, se ejecutaron las pruebas, las cuales fueron bastante positivas. Para todos los documentos validados se obtuvo un resultado *TOTAL_PASSED* lo que indica que la firma es válida, tal y como se esperaba.

Para el escenario 2, se utilizaron los documentos que fueron creados para el primer escenario, pero se modificó la política de diferentes maneras con el propósito de validar si la aplicación identifica como inválidos los documentos que no cumplen con las restricciones de firma. Por ejemplo, normalmente por medio de la política la aplicación identifica como válido un documento que incluye una firma generada con un certificado cuyo uso es el de "firma digital" y "no repudio", sin embargo, se modificó la política apropiadamente para que la "firma digital" no sea un uso válido del certificado de firma y se procedió a validar el documento. Por medio de esta modificación en la política, la aplicación identificó como inválido un documento que anteriormente era considerado válido, lo cual permite validar que la aplicación efectivamente valida las restricciones de la política para identificar documentos inválidos. Este tipo de modificación en la política se llevó a cabo para las siguientes restricciones: los algoritmos de firma válidos, los algoritmos *hash* permitidos, los usos de certificados, la cadena de certificados de confianza y el perfil de firma oficial. Para todos los casos la aplicación logró identificar que el documento validado no cumplía con la restricción que había sido modificada convenientemente. Los resultados variaron dependiendo del tipo de restricción que se modificó, tal y como se indica en el estándar ETSI EN 319 102-1 [26]. Por ejemplo, se obtuvo un resultado *TOTAL_FAILED* si el uso del certificado de firma es inválido, pero se obtuvo *TOTAL_PASSED* y mensajes de advertencia sobre la validez del documento si el algoritmo de encriptación utilizado para generar la firma no es aceptado, y así sucesivamente.

También, para la validación del escenario 2 se utilizaron documentos firmados que fueron alterados después de la firma. Para estos casos la aplicación logró identificar exitosamente un problema de integridad en el documento. Para la firma retornó un *TOTAL_PASSED*, ya

que la firma es válida, e indicó como parte de los resultados que la firma solamente cubre una parte del documento.

Para el escenario 3 se crearon documentos PDF y se firmaron con el formato PKCS#7. En todos los casos la aplicación retornó un *TOTAL_FAILED* e indicó que el formato de firma no es válido.

Las pruebas realizadas se muestran En el Apéndice E. Pruebas funcionales de la aplicación. Para cada una de las pruebas se puede consultar el escenario de prueba al que pertenece y las entradas y salidas de la aplicación.

Cada uno de los documentos utilizados para las pruebas también se validó con la herramienta Adobe Reader DC, para comparar los resultados con los de la aplicación desarrollada. Adobe Reader DC es la herramienta recomendada en el SNCD para la firma y validación del formato PAdES [24]. En la **Tabla 13** se muestra una comparación de los resultados obtenidos con las aplicaciones.

Tabla 13. Comparación de resultados obtenidos con la aplicación desarrollada y Adobe Reader DC

Documento	Resultado de la aplicación	Resultado de Adobe
Documentos válidos	Las firmas de los documentos se identificaron como válidas.	Las firmas de los documentos se identificaron como válidas.
Documentos inválidos (con problema de integridad)	Se detectó que los documentos fueron modificados después de la firma.	Se detectó que los documentos fueron modificados después de la firma.
Documentos inválidos (por incumplimiento de la política)	Las firmas de los documentos se detectaron como inválidas y se identificó la restricción de la política de validación que no cumplieron.	Las firmas de los documentos se identificaron como válidas, porque en Adobe Reader no fue posible establecer una política de validación con las restricciones de firma digital del SNCD.
Documentos con formato desconocido	Los documentos se detectaron como inválidos, ya que no cumplen con la restricción del formato de firma oficial (PAdES).	Los documentos se identificaron como válidos, porque en Adobe Reader no fue posible establecer una política de validación para restringir el formato de firma válido en el SNCD.

En resumen, la aplicación se comportó correctamente para los escenarios de pruebas definidos en el proyecto, ya que logró validar correctamente los documentos que se le presentaron en todas las pruebas. Por medio de esta validación de la aplicación se logró determinar que la funcionalidad base de la aplicación está funcionando correctamente. En un futuro es necesario realizar pruebas exhaustivas de la aplicación, de manera que cubran todos los posibles escenarios de restricciones de la política de firma según la legislación nacional.

6.2. Validaciones de seguridad de la aplicación

En la presente sección se muestran los resultados de la validación de la aplicación desde el punto de vista de seguridad. Primero se presentan los resultados del análisis estático de la aplicación y posteriormente los resultados de evaluarla con una guía de requerimientos técnicos para el aseguramiento de aplicaciones de certificados y firma digital.

6.2.1. Validación de la aplicación con herramientas de análisis estático de seguridad

En esta sección se presentan los resultados de validar el código de la aplicación con herramientas de análisis estático de seguridad.

Es muy común que el resultado del análisis de seguridad de una aplicación varíe según la herramienta utilizada para validarla, por lo que se utilizaron tres herramientas distintas con el fin de que el análisis de la aplicación fuera más completo. Las herramientas que se utilizaron son:

- Security Code Scan
- Puma Scan Pro
- VisualCodeGrepper

En total se analizaron aproximadamente 36550 líneas de código de la aplicación. En la **Figura 16** se muestra un reporte tomado de VisualCodeGreeper sobre el código analizado.

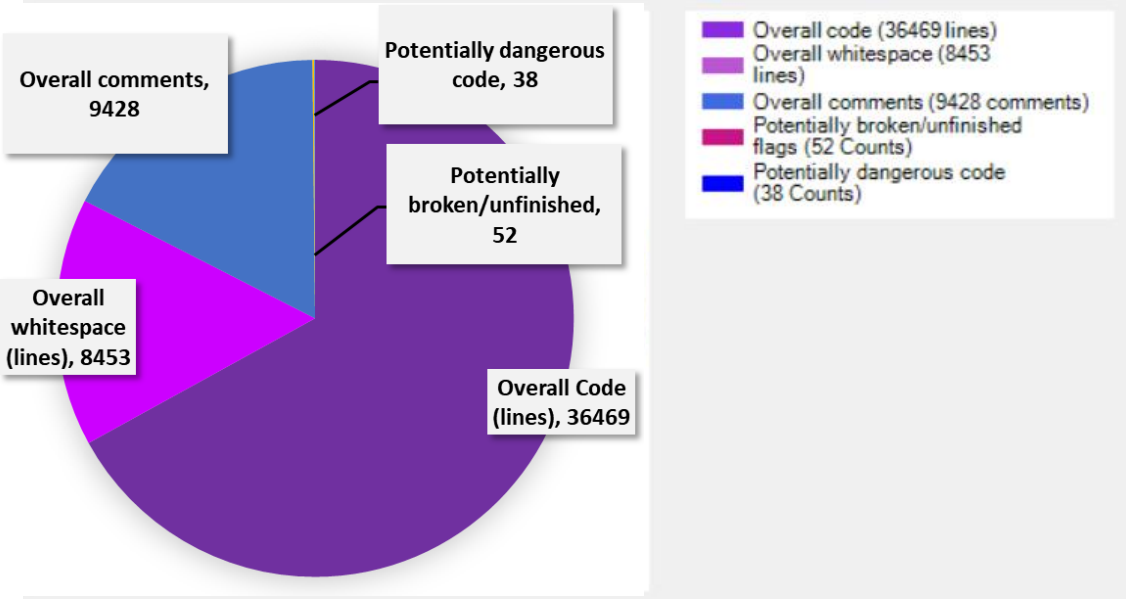

Figura 16. Reporte de la herramienta VisualCodeGreeper sobre el código analizado.

Las aplicaciones Security Code Scan y Puma Scan Pro no encontraron vulnerabilidades. La aplicación VisualCodeGrepper encontró 38 posibles problemas de seguridad, los cuales después de analizarlos resultaron en falsos positivos. En la **Tabla 14** se presentan las vulnerabilidades encontradas en orden de severidad y posteriormente se explica por qué son falsos positivos.

Tabla 14. Vulnerabilidades de la aplicación encontradas por la herramienta VisualCodeGrepper

Tipo	Severidad	Vulnerabilidad	Cantidad
1	Media	Almacenamiento inseguro de información sensible – contraseñas o llaves criptográficas privadas.	5
2	Media	Posible impacto en el rendimiento por *Thread lock* – 28 líneas de código en el bloque de *Thread lock.*	1
3	Normal	Operación con objetos numéricos de tipo Entero sin validación de *Integer Overflow.*	31
4	Baja	Posible impacto en el rendimiento por *Thread lock* – 9 líneas de código en el bloque de *Thread lock.*	1

Con la revisión detallada de los problemas de tipo 1, se determinó que son falsos positivos porque la información que se está almacenando no es sensible. Esta detección se dio, para

todos los casos, porque el nombre de la variable utilizada para almacenar la información contiene la palabra *Key*. Por ejemplo, *keyLength* que se utiliza para almacenar la longitud de una llave, pero no la llave propiamente:

```
String keyLength = "?";
 if (issuerPublicKey != null)
 {
     keyLength = getPublicKeySize(issuerPublicKey).ToString();
 }
 return keyLength;
```

En el caso de los problemas de seguridad de tipo 2 y 4, los *Thread lock* identificados se utilizan para evitar que dos o más procesos accedan a un recurso al mismo tiempo. Después de analizarlos se determinó que no tienen un impacto negativo en el rendimiento y que más bien el bloqueo es necesario para evitar que el proceso falle.

Los problemas de tipo 3 se detectaron en todos los bloques de código de tipo *for* como el que se muestra a continuación:

```
for (int a = 0; a < seq.Count; a++)
```

El posible *Integer Overflow* se podría dar si a la variable “a” se le asigna un valor mayor al máximo valor permitido para el tipo de dato Entero (Integer). Sin embargo, en ninguno de los casos va a ocurrir, ya que la condición “a < seq.Count” no lo permite. Esta condición verifica que la variable “a” siempre tenga un valor menor (<) que la variable de la derecha que también es de tipo Entero, por lo que el iterador “a++” nunca va a ser ejecutado cuando “a” tenga el valor máximo permitido en un Entero.

En resumen, con base en estos tres análisis estáticos de seguridad no se encontraron problemas reales de seguridad en la aplicación. Después de una revisión detallada de las vulnerabilidades identificadas en el código para realizar cualquier corrección, se determinó que todas eran falsos positivos.

En la siguiente sección se presenta la validación de la aplicación con la guía sobre requerimientos técnicos para el aseguramiento de una aplicación de firma digital.

6.2.2. Evaluación de la aplicación con base en la guía de requerimientos técnicos para el aseguramiento de aplicaciones de certificados y firma digital

En la presente sección se describen los resultados de aplicar la "*Guía de requerimientos técnicos para el aseguramiento de la información de los componentes tecnológicos que utilizan certificados y firma digital en aplicaciones de software dentro del Sistema Nacional de Certificación Digital"* [18] para validar la aplicación desde el punto de vista de seguridad y determinar si es confiable su uso dentro del SNCD.

La guía incluye políticas de seguridad para cuatro escenarios de uso:

- Creación de firma digital y/o sello electrónico.
- Verificación de firma digital y/o sello electrónico.
- Autenticación de usuarios mediante certificados digitales.
- Conversión de una firma digital en formato simple a formato avanzado.

La aplicación desarrollada solamente implementa el escenario de uso de **verificación de firma digital y/o sello electrónico**. Por lo tanto, para evaluar la aplicación se extrajeron y evaluaron solamente las políticas de seguridad de **verificación de firma digital y/o sello electrónico**.

En total se evaluaron 20 políticas de seguridad, de las cuales:

- 10 se cumplen en la aplicación
- 10 no aplican en el contexto de desarrollo de la aplicación.

En el caso de las políticas que no aplican en el contexto de desarrollo de la aplicación, se debe a dos motivos principalmente:

1) El control relacionado con la política se debe implementar a nivel de infraestructura, por lo que la política queda fuera del alcance de la aplicación.

2) Por el tipo de la aplicación no es necesario implementar el control de seguridad relacionado con la política.

Un ejemplo del primer motivo se presenta en la **Figura 17**. El objetivo de control de la política 37 está fuera del contexto de desarrollo la aplicación y se relaciona directamente con la infraestructura donde va a ser ejecutada la aplicación.

No.	Política de Seguridad	Objetivos de Control	Cumplimiento
37	Se debe proteger el documento electrónico cuyas firmas se van a verificar, mientras transita por la memoria local, de manera que no pueda ser modificado por usuarios no autorizados.	4	N/A

No.	Objetivo de control
4	Se debe validar que las máquinas en las cuales se ejecutan componentes de la aplicación están libres de virus, malware y cualquier otro tipo de software malicioso que facilite la modificación no autorizada de datos.

Figura 17. Ejemplo de política de infraestructura

Un ejemplo del segundo caso se presenta en la política 33, en ésta se establece que “Se debe proteger el resultado de la validación del documento electrónico cuyas firmas se van a verificar, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.”. Sin embargo, la aplicación desarrollada es de tipo consola y los resultados de la validación de un documento se almacenan localmente en la máquina donde se ejecuta el programa, nunca se transmiten por una red. Por lo tanto, la política no aplica. Esta política es ideal para aplicaciones de tipo *web* o distribuidas.

En relación con las políticas de seguridad que se cumplen con la aplicación, se brinda una observación para cada una de ellas sobre cómo se implementan los objetivos de control en la aplicación.

Los resultados de la evaluación de la aplicación se presentan en el Apéndice F. Resultados de la evaluación de las políticas de seguridad para aplicaciones de verificación de firma

digital y sello electrónico en la aplicación desarrollada. Para todas las políticas se especifica si la aplicación evaluada cumple o no con la política, o si no aplica en el contexto de la aplicación. También, se brinda una observación sobre el resultado. Adicionalmente, con el fin de facilitar la comprensión de la funcionalidad que se incluye en la aplicación, en el Apéndice G. Objetivos de control para las políticas de verificación de firma digital y/o sello electrónico, se muestra la lista de los objetivos de control. Por ejemplo, si la aplicación cumple con la política X quiere decir que la aplicación implementa un mecanismo como el que se detalla en el objetivo de control relacionado con la política X.

En resumen, la aplicación cumple con todas las políticas que aplican para el contexto de la aplicación. La evaluación de la aplicación con la guía permitió determinar que tiene un nivel adecuado de aseguramiento de la información, ya que cumple con los requerimientos técnicos correspondientes para la verificación de firma digital.

7. Conclusiones y trabajo futuro

En este capítulo se presentan las conclusiones de este proyecto y el posible trabajo futuro.

7.1. Conclusiones

La revisión sistemática de las leyes y reglamentos de Costa Rica para la firma digital de documentos permitió identificar que los perfiles CAdES X-L, PAdES LTV y XAdES X-L de los estándares europeos de la ETSI, son los perfiles oficiales de firma digital de documentos dentro del SNCD. Posteriormente, una valoración de las características de estos estándares, con respecto a los requerimientos de firma digital de la regulación del SNCD, permitió determinar que los requerimientos técnicos de la legislación de Costa Rica se basan en estos estándares.

A partir del análisis y caracterización de los estándares oficiales, se seleccionó el formato PAdES LTV para desarrollar una aplicación que permita validarlo. Mediante una revisión de las guías y herramientas oficiales dentro del SNCD para la validación de los formatos, se determinó que no hay disponible una aplicación propia del SNCD que valide este tipo de formato. Una aplicación oficial de este tipo sería muy útil para que las entidades que implementen firma digital puedan utilizarla en sus desarrollos.

Tomando como insumos los requerimientos obtenidos directamente de los estándares europeos de la ETSI y la librería DSS que la Unión Europea tiene a disposición para validar estos estándares, se desarrolló la aplicación “Validador de formato de firma PAdES LTV”. La librería DSS sigue todos los lineamientos europeos para la validación de este formato, por lo que se migró para utilizarla en la aplicación. Por medio del uso de esta librería y el desarrollo de la aplicación con base en la especificación técnica de los estándares de la ETSI se logró construir una aplicación segura y robusta desde el punto de vista funcional, que podría ser tomada en cuenta por los encargados de la implementación de firma digital dentro del SNCD para que forme parte de las herramientas de ejemplo disponibles para la firma y validación de documentos.

Para determinar si realmente la aplicación es eficaz en la validación de documentos, se definieron escenarios de prueba funcionales para validarla. La aplicación validó e identificó correctamente documentos válidos, inválidos y con formatos de firma desconocidos. Aunque las pruebas no cubrieron toda la funcionalidad de la aplicación, permiten determinar que la funcionalidad base de la aplicación esta correcta. Estos escenarios pueden utilizarse como un punto de partida para eventualmente certificar que la aplicación valida correctamente cualquier documento firmado digitalmente con el formato PAdES LTV en el SNCD.

En relación con la seguridad de la aplicación desarrollada, se analizó con herramientas de análisis estático de seguridad y se evaluó con una guía de requerimientos técnicos para el aseguramiento de aplicaciones de firma digital. De igual manera este análisis sirve de base para determinar que la aplicación tiene un nivel apropiado de seguridad.

7.2. Trabajo futuro

La aplicación desarrollada durante este proyecto de investigación debe ser validada por expertos encargados de la implementación de firma digital en el país, antes de que pueda utilizarse dentro del SNCD. Aunque la aplicación se desarrolló siguiendo los requerimientos de los estándares europeos y fue efectiva validando los documentos durante las pruebas funcionales, no es posible asegurar que puede validar cualquier documento PDF firmado. Se deben realizar más casos de prueba y se debe llevar a cabo una valoración experta de los requerimientos que se extrajeron de los estándares y de la aplicación de ejemplo (DSS). Además, es necesario certificar que la aplicación cumple con los requisitos de seguridad propuestos dentro del SNCD. Durante este proyecto, la aplicación se validó desde el punto de vista de seguridad por medio de herramientas de análisis estático y de una evaluación con la guía de aseguramiento propuesta el señor Alejandro Mora. Sin embargo, al momento de la investigación estas herramientas no constituyen medios oficiales dentro del SNCD para certificar una aplicación de *software* de firma digital. Aunque no se encontraron problemas

de seguridad en la aplicación, se debe someter a un proceso oficial de revisión de seguridad del SNCD que certifique que tiene un nivel apropiado de seguridad.

Directamente en la aplicación se implementan muchos controles de seguridad. Sin embargo, para determinar si el documento que se va a validar está libre de código malicioso es necesario analizarlo previamente con un antivirus. Por lo tanto, se propone desarrollar dentro de la aplicación la funcionalidad de este mecanismo de control, de manera que sea la misma aplicación la que verifique si el documento contiene o no código malicioso antes de analizarlo.

La aplicación desarrollada valida solamente el formato PAdES. Sin embargo, está programada de manera que se pueda agregar fácilmente la funcionalidad de validación de los otros formatos. Por lo tanto, se sugiere agregar soporte de validación de los otros perfiles oficiales de los formatos de firma avanzada, CAdES X-L y XAdES X-L de manera que la validación de todos los formatos se pueda realizar con una misma herramienta.

Por último, la versión de la guía de aseguramiento utilizada durante la validación de seguridad de la aplicación no es la versión final, ya que se encontraba en desarrollo durante este proyecto. Cuando esté disponible la versión final se sugiere aplicarla nuevamente para validar la aplicación.

8. Bibliografía

[1] Gobierno de Costa Rica, Masificación de la implementación y el uso de la firma digital en el sector público costarricense, Diario Oficial La Gaceta, 2014.

[2] Dirección de Certificadores de Firma Digital, Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente, MICITT, 2013.

[3] Asamblea Legislativa de la República de Costa Rica, Ley de Certificados, Firmas Digitales y Documentos Electrónicos, Diario Oficial La Gaceta, 2005.

[4] Dirección de Certificadores de Firma Digital, Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, MICITT, 2006.

[5] Dirección de Certificadores de Firma Digital, Política de certificados para la jerarquía nacional de certificadores registrados, MICITT, 2013.

[6] Dirección de Certificadores de Firma Digital, Política de sellado de tiempo del Sistema Nacional de Certificación Digital, MICITT, 2008.

[7] H. Tipton, Official (ISC)2 Guide to the CISSP CBK, Second Edition, Auerbach Publications; 2 edition, 2009.

[8] J. A. Buchmann, E. Karatsiolis and A. Wiesmaier, Introduction to Public Key Infrastructures, Berlin, Heidelberg: Springer, 2013.

[9] R. Shirey, Security architecture for internet protocols. A Guide for Protocol Designs and Standards, Internet Engineering Task Force, 1994.

[10] M. Bishop, Computer Security: Art and Science, Addison Wesley, 2002.

[11] ISO, All about ISO. Obtenido de ISO.org: https://www.iso.org/about-us.html, ISO, 2018.

[12] ETSI, About ETSI. Obtenido de ETSI.org: https://www.etsi.org/index.php/about, ETSI, 2017.

[13] ETSI, ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), ETSI, 2012.

[14] ETSI, ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES), ETSI, 2006.

[15] ETSI, ETSI TS 102 778-1: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES, ETSI, 2009.

[16] CEF Digital, Start using Digital Signature Services (DSS). Obtenido de ec.europa.eu: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773260, CEF Digital, 2018.

[17] OWASP, Source Code Analysis Tools de owasp.org: https://www.owasp.org/index.php/Source_Code_Analysis_Tools, OWASP, 2019.

[18] A. M. Castro, Guía de requerimientos técnicos para el aseguramiento de la información de los componentes tecnológicos que utilizan certificados y firma digital en aplicaciones de software dentro del Sistema Nacional de Certificación Digital, UCR, 2017.

[19] A. M. Castro, Definición de un proceso de aseguramiento de la información para los componentes tecnológicos que utilizan certificados y firma digital en una aplicación de software dentro del Sistema Nacional de Certificación Digital, UCR, 2017.

[20] ETSI, ETSI TS 102 176-1: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, ETSI, 2007.

[21] Dirección de Certificadores de Firma Digital, Guía de Firma Digital para XólidoSign, MICITT, 2013.

[22] Dirección de Certificadores de Firma Digital, Guía de Firma Digital para Adobe Reader XI., MICITT, 2014.

[23] Dirección de Certificadores de Firma Digital, Guía de Firma Digital para Adobe Reader XI en Mac., MICITT, 2014.

[24] Dirección de Certificadores de Firma Digital, Guía de Firma Digital para Adobe Reader DC., MICITT, 2015.

[25] Adobe Systems Incorporated, ISO 32000-1: "Document management - Portable document format - Part 1: PDF 1.7", Adobe Systems Incorporated, 2008.

[26] ETSI, ETSI EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, ETSI, 2015.

[27] ETSI, ETSI TS 102 778-2: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1, ETSI, 2009.

[28] ETSI, ETSI TS 102 778-3: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles, ETSI, 2010.

[29] ETSI, ETSI TS 102 778-4: Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile, ETSI, 2009.

[30] BouncyCastle, About BouncyCastle. Obtenido de bouncycastle.org: https://www.bouncycastle.org/, BouncyCastle, 2017.

[31] iText, About us. Obtenido de itextpdf.com: https://itextpdf.com/en/about-us, iText, 2018.

[32] ETSI, Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1, ETSI, 2009.

9. Apéndices

9.1. Apéndice A. Características de los formatos oficiales de firma digital dentro del SNCD.

En este apéndice se presentan las características extraídas de los formatos oficiales de firma digital dentro del SNCD. Estas características se extrajeron para utilizarlas como criterios de selección de al menos un formato para validarlo con la aplicación. En la **Tabla 15** se muestra la primera parte del listado de características y la segunda parte en la **Tabla 16**.

Tabla 15. Lista de características extraídas de los formatos oficiales de firma digital en el SNCD. 1ra parte.

Formato	Tipo de archivo	Tipos de firma	Otros formatos requeridos	Requiere de librerías de terceros para su implementación	Librerías requeridas	Requiere implementar algún otro formato	Nivel de complejidad de desarrollo
XAdES	XML	*Enveloped, enveloping y detached*	CAdES	Si	BouncyCastle	Si	Media
CAdES	Binario	*Enveloped, enveloping y detached*	-	Si	BouncyCastle	No	Media
PAdES	PDF	*Enveloped*	CAdES	Si	BouncyCastle y librería archivos PDF	Si	Alta

Tabla 16. Lista de características extraídas de los formatos oficiales de firma digital en el SNCD. 2da parte.

Formato	Tiempo de desarrollo	Está disponible una aplicación firmar con el formato	Está disponible una aplicación para validar el formato	Existe una guía de desarrollo oficial	Usos	Usuarios	Utilidad
XAdES	Medio	Si	Si	Si	Para firmar cualquier tipo de archivo y transacciones electrónicas. Se caracteriza por proveer interoperabilidad entre sistemas.	Sistemas	Alta
CAdES	Medio	No, solo de terceros	No, solo de terceros	No, solo guías para utilizar las herramientas de terceros	Para firmar archivos en formato binario	Sistemas	Media
PAdES	Alto	No, solo de terceros	No, solo de terceros	No, solo guías para utilizar las herramientas de terceros	Para firmar documentos PDF.	Personas	Alta

9.2. Apéndice B. Política de validación de firma de la aplicación

En el presente apéndice se muestra la política de validación de firma utilizada en la aplicación para este proyecto, resaltado en negrita los elementos que fueron identificados en la regulación nacional.

```
<ConstraintsParameters Name="Politica SNCD"
xmlns="http://dss.esig.europa.eu/validation/policy">
        <Description>Valida firmas electronicas e indica si son firmas avanzadas. Todos los
certificados y sus cadenas de certificados son validados. Esto incluye validacion de CRLs, OCSP y
estampas de tiempo.
        </Description>
        <SignatureConstraints>
                <AcceptablePolicies Level="FAIL">
                        <Id>ANY_POLICY</Id>
                        <Id>NO_POLICY</Id>
                </AcceptablePolicies>
                <PolicyAvailable Level="FAIL" />
                <PolicyHashMatch Level="FAIL" />
                <AcceptableFormats Level="FAIL">
                        <Id>CAdES_BASELINE_T</Id>
                </AcceptableFormats>
                <BasicSignatureConstraints>
                        <ReferenceDataExistence Level="FAIL" />
                        <ReferenceDataIntact Level="FAIL" />
                        <SignatureIntact Level="FAIL" />
                        <ProspectiveCertificateChain Level="FAIL" />
                        <TrustedServiceTypeIdentifier Level="WARN">
                                <Id>CERT</Id>
                        </TrustedServiceTypeIdentifier>
                        <TrustedServiceStatus Level="FAIL">
                                <Id>OK</Id>
                        </TrustedServiceStatus>
                        <SigningCertificate>
                                <Recognition Level="FAIL" />
                                <Signature Level="FAIL" />
                                <NotExpired Level="WARN" />
                                <RevocationDataAvailable Level="FAIL" />
                                <RevocationDataNextUpdatePresent Level="WARN" />
                                <RevocationDataFreshness Level="INFORM" />
                                <KeyUsage Level="WARN">
```

```
                    <Id>nonRepudiation</Id>
                    <Id>digitalSignature</Id>
                </KeyUsage>
                <NotRevoked Level="FAIL" />
                <NotOnHold Level="FAIL" />
                <Qualification Level="INFORM" />
                <SupportedByQSCD Level="INFORM" />
                <IssuedToLegalPerson Level="INFORM" />
                <Cryptographic Level="FAIL">
                    <AcceptableEncryptionAlgo>
                    <Algo>RSA</Algo>
                    <Algo>DSA</Algo>
                    <Algo>ECDSA</Algo>
                </AcceptableEncryptionAlgo>
                <MiniPublicKeySize>
                    <Algo Size="128">DSA</Algo>
                    <Algo Size="1024">RSA</Algo>
                    <Algo Size="192">ECDSA</Algo>
                </MiniPublicKeySize>
                <AcceptableDigestAlgo>
                    <Algo>SHA1</Algo>
                    <Algo>SHA224</Algo>
                    <Algo>SHA256</Algo>
                    <Algo>SHA384</Algo>
                    <Algo>SHA512</Algo>
                    <Algo>RIPEMD160</Algo>
                </AcceptableDigestAlgo>
                </Cryptographic>
            </SigningCertificate>
            <CACertificate>
                <Signature Level="FAIL" />
                <NotExpired Level="FAIL" />
                <RevocationDataAvailable Level="FAIL" />
                <RevocationDataNextUpdatePresent Level="WARN" />
                <RevocationDataFreshness Level="INFORM" />
                <NotRevoked Level="FAIL" />
                <NotOnHold Level="FAIL" />
                <Cryptographic Level="FAIL">
                    <AcceptableEncryptionAlgo>
                    <Algo>RSA</Algo>
                    <Algo>DSA</Algo>
                    <Algo>ECDSA</Algo>
                </AcceptableEncryptionAlgo>
                <MiniPublicKeySize>
```

```
                        <Algo Size="128">DSA</Algo>
                        <Algo Size="1024">RSA</Algo>
                        <Algo Size="192">ECDSA</Algo>
                    </MiniPublicKeySize>
                    <AcceptableDigestAlgo>
                        <Algo>SHA1</Algo>
                        <Algo>SHA224</Algo>
                        <Algo>SHA256</Algo>
                        <Algo>SHA384</Algo>
                        <Algo>SHA512</Algo>
                        <Algo>RIPEMD160</Algo>
                    </AcceptableDigestAlgo>
                    </Cryptographic>
            </CACertificate>
            <Cryptographic Level="FAIL">
                    <AcceptableEncryptionAlgo>
                        <Algo>RSA</Algo>
                        <Algo>DSA</Algo>
                        <Algo>ECDSA</Algo>
                    </AcceptableEncryptionAlgo>
                    <MiniPublicKeySize>
                        <Algo Size="128">DSA</Algo>
                        <Algo Size="1024">RSA</Algo>
                        <Algo Size="192">ECDSA</Algo>
                    </MiniPublicKeySize>
                    <AcceptableDigestAlgo>
                        <Algo>SHA1</Algo>
                        <Algo>SHA224</Algo>
                        <Algo>SHA256</Algo>
                        <Algo>SHA384</Algo>
                        <Algo>SHA512</Algo>
                        <Algo>RIPEMD160</Algo>
                    </AcceptableDigestAlgo>
            </Cryptographic>
    </BasicSignatureConstraints>
    <SignedAttributes>
            <SigningCertificatePresent Level="FAIL" />
            <SigningCertificateSigned Level="FAIL" />
            <CertDigestPresent Level="FAIL" />
            <CertDigestMatch Level="FAIL" />
            <IssuerSerialMatch Level="INFORM" />
            <SigningTime Level="FAIL" />
    </SignedAttributes>
    <UnsignedAttributes>
```

```
        </UnsignedAttributes>
</SignatureConstraints>
<Timestamp>
        <TimestampDelay Level="FAIL" Unit="DAYS" Value="30" />
        <MessageImprintDataFound Level="FAIL" />
        <MessageImprintDataIntact Level="FAIL" />
        <RevocationTimeAgainstBestSignatureTime      Level="FAIL" />
        <BestSignatureTimeBeforeIssuanceDateOfSigningCertificate Level="FAIL" />
        <SigningCertificateValidityAtBestSignatureTime Level="FAIL" />
        <AlgorithmReliableAtBestSignatureTime Level="FAIL" />
        <Coherence Level="WARN" />
        <BasicSignatureConstraints>
                <ReferenceDataExistence Level="FAIL" />
                <ReferenceDataIntact Level="FAIL" />
                <SignatureIntact Level="FAIL" />
                <ProspectiveCertificateChain Level="WARN" />
                <TrustedServiceTypeIdentifier Level="WARN">
                        <Id>CERT</Id>
                </TrustedServiceTypeIdentifier>
                <TrustedServiceStatus Level="WARN">
                        <Id>OK</Id>
                </TrustedServiceStatus>
                <SigningCertificate>
                        <Recognition Level="FAIL" />
                        <Signature Level="FAIL" />
                        <NotExpired Level="FAIL" />
                        <RevocationDataAvailable Level="FAIL" />
                        <RevocationDataNextUpdatePresent Level="WARN" />
                        <RevocationDataFreshness Level="INFORM" />
                        <NotRevoked Level="FAIL" />
                        <NotOnHold Level="FAIL" />
                        <Cryptographic Level="FAIL">
                                <AcceptableEncryptionAlgo>
                                        <Algo>RSA</Algo>
                                        <Algo>DSA</Algo>
                                        <Algo>ECDSA</Algo>
                                </AcceptableEncryptionAlgo>
                                <MiniPublicKeySize>
                                        <Algo Size="128">DSA</Algo>
                                        <Algo Size="1024">RSA</Algo>
                                        <Algo Size="192">ECDSA</Algo>
                                </MiniPublicKeySize>
                                <AcceptableDigestAlgo>
                                        <Algo>SHA1</Algo>
```

```
                    <Algo>SHA224</Algo>
                    <Algo>SHA256</Algo>
                    <Algo>SHA384</Algo>
                    <Algo>SHA512</Algo>
                    <Algo>RIPEMD160</Algo>
                </AcceptableDigestAlgo>
            </Cryptographic>
        </SigningCertificate>
        <CACertificate>
            <Signature Level="FAIL" />
            <NotExpired Level="FAIL" />
            <RevocationDataAvailable Level="WARN" />
            <RevocationDataNextUpdatePresent Level="WARN" />
            <RevocationDataFreshness Level="INFORM" />
            <NotRevoked Level="FAIL" />
            <NotOnHold Level="FAIL" />
            <Cryptographic Level="FAIL">
                <AcceptableEncryptionAlgo>
                    <Algo>RSA</Algo>
                    <Algo>DSA</Algo>
                    <Algo>ECDSA</Algo>
                </AcceptableEncryptionAlgo>
                <MiniPublicKeySize>
                    <Algo Size="128">DSA</Algo>
                    <Algo Size="1024">RSA</Algo>
                    <Algo Size="192">ECDSA</Algo>
                </MiniPublicKeySize>
                <AcceptableDigestAlgo>
                    <Algo>SHA1</Algo>
                    <Algo>SHA224</Algo>
                    <Algo>SHA256</Algo>
                    <Algo>SHA384</Algo>
                    <Algo>SHA512</Algo>
                    <Algo>RIPEMD160</Algo>
                </AcceptableDigestAlgo>
            </Cryptographic>
        </CACertificate>
        <Cryptographic Level="FAIL">
            <AcceptableEncryptionAlgo>
                <Algo>RSA</Algo>
                <Algo>DSA</Algo>
                <Algo>ECDSA</Algo>
            </AcceptableEncryptionAlgo>
            <MiniPublicKeySize>
```

```
                                <Algo Size="128">DSA</Algo>
                                <Algo Size="1024">RSA</Algo>
                                <Algo Size="192">ECDSA</Algo>
                        </MiniPublicKeySize>
                        <AcceptableDigestAlgo>
                                <Algo>SHA1</Algo>
                                <Algo>SHA224</Algo>
                                <Algo>SHA256</Algo>
                                <Algo>SHA384</Algo>
                                <Algo>SHA512</Algo>
                                <Algo>RIPEMD160</Algo>
                        </AcceptableDigestAlgo>
                </Cryptographic>
        </BasicSignatureConstraints>
</Timestamp>
<Revocation>
        <RevocationFreshness Level="FAIL" Unit="DAYS" Value="30" />
        <BasicSignatureConstraints>
                <ReferenceDataExistence Level="FAIL" />
                <ReferenceDataIntact Level="FAIL" />
                <SignatureIntact Level="FAIL" />
                <ProspectiveCertificateChain Level="WARN" />
                <TrustedServiceTypeIdentifier Level="WARN">
                        <Id>CERT</Id>
                </TrustedServiceTypeIdentifier>
                <TrustedServiceStatus Level="WARN">
                        <Id>OK</Id>
                </TrustedServiceStatus>
                <SigningCertificate>
                        <Recognition Level="FAIL" />
                        <Signature Level="FAIL" />
                        <NotExpired Level="FAIL" />
                        <RevocationDataAvailable Level="FAIL" />
                        <RevocationDataNextUpdatePresent Level="WARN" />
                        <RevocationDataFreshness Level="INFORM" />
                        <NotRevoked Level="FAIL" />
                        <NotOnHold Level="FAIL" />
                        <Cryptographic Level="WARN">
                                <AcceptableEncryptionAlgo>
                                        <Algo>RSA</Algo>
                                        <Algo>DSA</Algo>
                                </AcceptableEncryptionAlgo>
                                <MiniPublicKeySize>
                                        <Algo Size="128">DSA</Algo>
```

```
                    <Algo Size="1024">RSA</Algo>
                    <Algo Size="192">ECDSA</Algo>
                </MiniPublicKeySize>
                <AcceptableDigestAlgo>
                    <Algo>SHA1</Algo>
                    <Algo>SHA224</Algo>
                    <Algo>SHA256</Algo>
                    <Algo>SHA384</Algo>
                    <Algo>SHA512</Algo>
                    <Algo>RIPEMD160</Algo>
                </AcceptableDigestAlgo>
            </Cryptographic>
        </SigningCertificate>
        <CACertificate>
            <Signature Level="FAIL" />
            <NotExpired Level="FAIL" />
            <RevocationDataAvailable Level="WARN" />
            <RevocationDataNextUpdatePresent Level="WARN" />
            <RevocationDataFreshness Level="INFORM" />
            <NotRevoked Level="FAIL" />
            <NotOnHold Level="FAIL" />
            <Cryptographic Level="FAIL">
                <AcceptableEncryptionAlgo>
                    <Algo>RSA</Algo>
                    <Algo>DSA</Algo>
                    <Algo>ECDSA</Algo>
                </AcceptableEncryptionAlgo>
                <MiniPublicKeySize>
                    <Algo Size="128">DSA</Algo>
                    <Algo Size="1024">RSA</Algo>
                    <Algo Size="192">ECDSA</Algo>
                </MiniPublicKeySize>
                <AcceptableDigestAlgo>
                    <Algo>SHA1</Algo>
                    <Algo>SHA224</Algo>
                    <Algo>SHA256</Algo>
                    <Algo>SHA384</Algo>
                    <Algo>SHA512</Algo>
                    <Algo>RIPEMD160</Algo>
                </AcceptableDigestAlgo>
            </Cryptographic>
        </CACertificate>
        <Cryptographic Level="FAIL">
            <AcceptableEncryptionAlgo>
```

```
                                        <Algo>RSA</Algo>
                                        <Algo>DSA</Algo>
                                        <Algo>ECDSA</Algo>
                                    </AcceptableEncryptionAlgo>
                                    <MiniPublicKeySize>
                                        <Algo Size="128">DSA</Algo>
                                        <Algo Size="1024">RSA</Algo>
                                        <Algo Size="192">ECDSA</Algo>
                                    </MiniPublicKeySize>
                                    <AcceptableDigestAlgo>
                                        <Algo>SHA1</Algo>
                                        <Algo>SHA224</Algo>
                                        <Algo>SHA256</Algo>
                                        <Algo>SHA384</Algo>
                                        <Algo>SHA512</Algo>
                                        <Algo>RIPEMD160</Algo>
                                    </AcceptableDigestAlgo>
                                </Cryptographic>
                            </BasicSignatureConstraints>
                        </Revocation>
                        <Cryptographic Level="FAIL">
                            <AcceptableEncryptionAlgo>
                                <Algo>RSA</Algo>
                                <Algo>DSA</Algo>
                                <Algo>ECDSA</Algo>
                            </AcceptableEncryptionAlgo>
                            <MiniPublicKeySize>
                                <Algo Size="128">DSA</Algo>
                                <Algo Size="1024">RSA</Algo>
                                <Algo Size="192">ECDSA</Algo>
                            </MiniPublicKeySize>
                            <AcceptableDigestAlgo>
                                <Algo>SHA1</Algo>
                                <Algo>SHA224</Algo>
                                <Algo>SHA256</Algo>
                                <Algo>SHA384</Algo>
                                <Algo>SHA512</Algo>
                                <Algo>RIPEMD160</Algo>
                            </AcceptableDigestAlgo>
                        </Cryptographic>
                    </ConstraintsParameters>
```

9.3. Apéndice C. Ejemplos de resultados de la aplicación

En este apéndice se muestra un ejemplo resumido de cada uno de los reportes de resultados de validación de firma de la aplicación desarrollada.

Reporte simple

```
<?xml version="1.0"?>
<SimpleReport xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="http://dss.esig.europa.eu/validation/simple-report">
  <Policy>
    <PolicyName>QES AdESQC TL based</PolicyName>
    <PolicyDescription>Valida firmas electronicas e indica si son firmas avanzadas.
          </PolicyDescription>
  </Policy>
  <ValidationTime>2019-04-29T00:47:42.6256655-06:00</ValidationTime>
  <DocumentName>DCFD-Política-de-Formato-Oficial-v1.0.pdf</DocumentName>
  <ValidSignaturesCount>1</ValidSignaturesCount>
  <SignaturesCount>1</SignaturesCount>
  <Signature Id="id-02D6F17D54ED1335C30BD7B2DDF834B5"
SignatureFormat="CAdES_BASELINE_T">
    <SignedBy>XXXXX XXXXXXX (FIRMA)</SignedBy>
    <CertificateChain>
      <Certificate>
        <id>A5E2AEE3B12BE7930EBC...</id>
        <qualifiedName> XXXXX XXXXXXX (FIRMA)</qualifiedName>
      </Certificate>
      <Certificate>
        <id>11C632ED91E174E822D8...</id>
        <qualifiedName>CA SINPE - PERSONA FISICA</qualifiedName>
      </Certificate>
    </CertificateChain>
    <SignatureLevel description="QESig">QESig</SignatureLevel>
    <Indication>TOTAL_PASSED</Indication>
    <Errors>The past signature validation is not conclusive!</Errors>
    <Errors>The result of the timestamps validation process is not conclusive!</Errors>
          …
    <SignatureScope name="Partial PDF" scope="PdfByteRangeSignatureScope">The document
byte range: [0, 513690, 563228, 2295]</SignatureScope>
  </Signature>
</SimpleReport>
```

Reporte detallado


```
<?xml version="1.0"?>
<DetailedReport xmlns="http://dss.esig.europa.eu/validation/detailed-report">
 <Signatures Id="id-02D6F17D54ED1335C...">
  <ValidationProcessBasicSignatures BestSignatureTime="2019-04-29T01:00:44-06:00">
   <Constraint Id="id-02D6F17D54ED1335C...">
    <Name NameId="ADEST_ROBVPIIC">Is the result conclusive?</Name>
    <Status>NOT OK</Status>
    <Error NameId="ADEST_ROBVPIIC_ANS">The result is not conclusive!</Error>
   </Constraint>
   <Conclusion>
    <Indication>INDETERMINATE</Indication>
    <Errors NameId="BBB_XCV_ICTIVRSC_ANS">The current time is not in the validity range
of the signer's certificate.</Errors>
   </Conclusion>
  </ValidationProcessBasicSignatures>
  <ValidationProcessTimestamps Id="6AF41189393790215324..."
Type="SIGNATURE_TIMESTAMP" ProductionTime="2013-05-20T13:48:47Z">
   <Constraint Id="6AF41189393790215324...">
    <Name NameId="ADEST_ROTVPIIC">Is the result conclusive?</Name>
    <Status>NOT OK</Status>
    <Error NameId="ADEST_ROTVPIIC_ANS">The result is not conclusive!</Error>
   </Constraint>
   <Conclusion>
    <Indication>INDETERMINATE</Indication>
    <Errors NameId="ADEST_ROTVPIIC_ANS">The result is not conclusive!</Errors>
   </Conclusion>
  </ValidationProcessTimestamps>
  <ValidationProcessLongTermData BestSignatureTime="2019-04-29T01:00:44">
   <Constraint>
    <Name NameId="LTV_ABSV">Is the result acceptable?</Name>
    <Status>OK</Status>
   </Constraint>
   ...
   <Conclusion>
    <Indication>INDETERMINATE</Indication>
   </Conclusion>
  </ValidationProcessLongTermData>
 </Signatures>
 <BasicBuildingBlocks Id="A5E2AEE3B12BE7930EBC..." Type="REVOCATION">
  <ISC>
   <Constraint>
```

```
      <Name NameId="BBB_ICS_ISCI">Is there an identified candidate for the signing
certificate?</Name>
       <Status>OK</Status>
      </Constraint>
      <Conclusion>
       <Indication>PASSED</Indication>
      </Conclusion>
      <CertificateChain>
       <ChainItem Id="11C632ED91E174E822D8...">
        <Source>TRUSTED_LIST</Source>
       </ChainItem>
      </CertificateChain>
    </ISC>
    <CV>
     ...
    </CV>
    <SAV>
     ...
    </SAV>
    <XCV>
     <Constraint>
      <Name NameId="BBB_XCV_CCCBB">Can the certificate chain be built till the trust
anchor?</Name>
       <Status>OK</Status>
     </Constraint>
     ...
    </XCV>
    <CertificateChain>
     <ChainItem Id="11C632ED91E174E822D8...">
      <Source>TRUSTED_LIST</Source>
     </ChainItem>
    </CertificateChain>
    <Conclusion>
     <Indication>PASSED</Indication>
    </Conclusion>
  </BasicBuildingBlocks>
  <BasicBuildingBlocks Id="6AF41189393790215324..." Type="TIMESTAMP">
   ...
  </BasicBuildingBlocks>
  <BasicBuildingBlocks Id="id-02D6F17D54ED1335C..." Type="SIGNATURE">
   ...
  </BasicBuildingBlocks>
</DetailedReport>
```

Información de diagnóstico


```
<?xml version="1.0"?>
<DiagnosticData xmlns="http://dss.esig.europa.eu/validation/diagnostic">
  <DocumentName>DCFD-Política-de-Formato-Oficial-v1.0.pdf</DocumentName>
  <ValidationDate>2019-04-29T01:00:44.0675028-06:00</ValidationDate>
  <Signatures>
    <Signature Id="id-02D6F17D54ED1335C30BD7B2DDF834B5">
      <SignatureFilename>DCFD-Política-de-Formato-Oficial-v1.0.pdf</SignatureFilename>
      <SignatureFormat>CAdES_BASELINE_T</SignatureFormat>
      <StructuralValidation />
      <BasicSignature>
      <EncryptionAlgoUsedToSignThisToken>RSA</EncryptionAlgoUsedToSignThisToken>
        <KeyLengthUsedToSignThisToken>2048</KeyLengthUsedToSignThisToken>
        <DigestAlgoUsedToSignThisToken>SHA256</DigestAlgoUsedToSignThisToken>
        <ReferenceDataFound>true</ReferenceDataFound>
        <ReferenceDataIntact>true</ReferenceDataIntact>
        <SignatureIntact>true</SignatureIntact>
        <SignatureValid>true</SignatureValid>
      </BasicSignature>
      <SigningCertificate Id="A5E2AEE3B12BE7930EBC..." />
      <CertificateChain>
        …
      </CertificateChain>
      <Timestamps>
            ...
      </Timestamps>
      <SignatureScopes>
        <SignatureScope name="Partial PDF" scope="PdfByteRangeSignatureScope">The document
byte range: [0, 513690, 563228, 2295]</SignatureScope>
      </SignatureScopes>
    </Signature>
  </Signatures>
  <UsedCertificates>
    <Certificate Id="A5E2AEE3B12BE7930EBC…">
      <SubjectDistinguishedName Format="CANONICAL">CN= XXXXX XXXXXXX
(FIRMA)...</SubjectDistinguishedName>
      <SerialNumber>-485315317777626817925612</SerialNumber>
      <CommonName> XXXXX XXXXXXX (FIRMA)</CommonName>
      ...
    </Certificate>
    …
  </UsedCertificates>
</DiagnosticData>
```

9.4. Apéndice D. Componentes de la aplicación

El presente apéndice muestra los componentes de la aplicación "Validador de formato de firma PAdES LTV" con sus respectivas entradas y salidas de información. En la **Tabla 17** se listan los componentes.

Tabla 17. Componentes de la aplicación con sus respectivas entradas y salidas de datos.

Componente	Descripción	Entradas	Salidas
Componente de interacción con el usuario o de conducción	Es el componente encargado de solicitarle al usuario la ruta del documento firmado digitalmente que se desea validar. También, se encarda de: • Leer el documento firmado. • Leer configuraciones de la aplicación como la política de validación. • Ejecutar el componente de validación (cuyos componentes se describen a continuación) • Guardar los resultados de la validación	• El documento firmado digitalmente	• Mensajes de la aplicación sobre los resultados de la validación del documento.
Validador de formato del documento	Este componente verifica que el formato de la firma cumpla con el formato PAdES. Las validaciones específicas LTV se realizan en el "Validador de aceptación de firma".	• Documento firmado digitalmente (incluye la firma)	• Si el formato de la firma está conforme al estándar PAdES retorna el indicador *PASSED*. • Caso contrario retorna *FAILED*.

Componente	Descripción	Entradas	Salidas
Identificador del certificado de firma	Componente responsable de identificar y extraer el certificado de firma que se utilizará para validar la firma.	• La firma digital • El documento firmado	• Si el certificado es extraído, retorna el certificado. • Si no puede ser identificado, retorna el indicador INDETERMINATE.
Inicializador del contexto de validación	Este componente inicializa todas las restricciones incluidas en la política de validación (criptográficas, de elementos de firma, entre otras), así como cualquier otra configuración que provee el componente de conducción, también conocido como componente de interacción con el usuario (orígenes de datos para la consulta de certificados, para llamadas OCSP, entre otras)	• La política de validación de firma. • Configuraciones • La firma digital • TSL	• Si la inicialización es exitosa retorna el indicador *PASSED*. • En caso de presentarse alguna falla retorna *INDETERMINATE* junto con el detalle del error.
Verificador de la información de revocación	Verifica que la información de revocación sea “fresca” en un momento dado de validación.	• Información de revocación (CRL o OCSP) • El certificado que se está validando. • El tiempo de la validación. • Restricciones de X.509.	• El indicador *PASSED* si la información de revocación es considerada “fresca”. • El indicador *FAILED* si no se considera “fresca”.

Componente	Descripción	Entradas	Salidas
Validador de X.509	Valida el certificado de firma. Entre otras cosas, realiza lo siguiente: • Valida el estado del certificado de firma para la fecha de validación. • Construye la cadena de certificados. • Valida la cadena de certificados • Verifica el estado de revocación de cada certificado • Verificación de la estampa de tiempo de la firma	• Certificado de firma. • Restricciones X.509 incluidas en la política de validación. • Restricciones criptográficas. • Otros certificados de la cadena de certificados (opcional).	• Si el certificado de firma y la cadena de certificados son válidos, retorna el indicador *PASSED.* • Cualquier otro caso retorna *INDETERMINATE* junto con un sub indicador del error de validación encontrado. Por ejemplo, si no fue posible crear la cadena de certificados, si el certificado está revocado, si una restricción de criptografía no se cumple, entre otros.
Verificador criptográfico	Este componente valida la integridad del documento firmado, por medio de verificaciones criptográficas.	• La firma digital • El certificado de firma. • El documento firmado	• Si la firma pasa la verificación criptográfica retorna *PASSED.* • Si no se puede obtener la parte del documento que fue firmado retorna un *INDETERMINATE.* • Retorna *FAILED* si la verificación de integridad falla, es decir, si el hash incluido en la firma no concuerda con el calculado.

Componente	Descripción	Entradas	Salidas
Validador de aceptación de firma	Realiza verificaciones adicionales, propias del perfil PAdES LTV. Por ejemplo, verificación de otras estampas de tiempo.	• La firma digital • Restricciones criptográficas	• El indicador de estado *PASSED* si las validaciones son exitosas. • Si alguna otra validación falla retorna *INDETERMINATE* junto con un detalle del error.
Componente de reporte de resultados	Este componente se encarga de general los tres resultados del proceso de validación de firma: • El reporte detallado • El reporte simple • Y la información de diagnóstico	Las salidas generadas por cada uno de los componentes durante el proceso de validación de la firma o firmas digitales incluidas en el documento.	Los reportes de resultados en formato XML: • El reporte detallado • El reporte simple • Y la información de diagnóstico

9.5. Apéndice E. Pruebas funcionales de la aplicación

En este apéndice se presentan las pruebas funcionales que fueron ejecutadas en la aplicación "Validador de formato de firma PAdES LTV", para validar si verifica correctamente el formato PAdES LTV. En la **Tabla 18** se listan las pruebas. Para cada prueba se indica el escenario de prueba al que pertenece y las respectivas entradas y salidas de la aplicación.

Tabla 18. Lista de pruebas funcionales ejecutadas en la aplicación.

Id	Esce-nario	Entradas		Salidas	
		Documento	**Política de validación de firma**	**Resultado**	**Observaciones**
1	1	CPSistemaNacionalCertificaciónDigitalversión1.pdf (tomado de la documentación del SNCD)	Se configuró de acuerdo con las restricciones del SNCD: *AcceptableFormats:* ***CAdES_BASELINE_T*** *SigningCertificate – KeyUsage:* ***nonRepudiation***, ***signature*** *AcceptableEncryptionAlgo:* ***RSA*** *AcceptableDigestAlgo:* ***SHA1***, ***SHA256***	*<Indication> TOTAL_PASSED </Indication>*	La aplicación generó un mensaje informativo, que indica que el certificado de la persona que firmó el documento ya venció. Sin embargo, esto no altera el resultado de la firma. Sigue siendo válida porque se generó cuando el certificado estaba vigente. *< Infos >* *The current time is not in the validity range of the signer's certificate.* *</ Infos >*

Id	Esce-nario	Entradas		Salidas	
		Documento	**Política de validación de firma**	**Resultado**	**Observaciones**
2	1	DCFD-Política-de-certificados-v1.1.pdf (tomado de la documentación del SNCD)	Se utilizó la misma configuración de la prueba 1. Siguiendo las restricciones de firma del SNCD.	*<Indication> TOTAL_PASSED </Indication>*	Se generaron los mismos mensajes de la prueba 1, los cuales indican que el certificado de la persona que firmó el documento ya venció.
3	1	DCFD-Política-de-Formato-Oficial-v1.0.pdf (tomado de la documentación del SNCD)	Se utilizó la misma configuración de la prueba 1. Siguiendo las restricciones de firma del SNCD.	*<Indication> TOTAL_PASSED </Indication>*	Se generaron los mismos mensajes de la prueba 1, los cuales indican que el certificado de la persona que firmó el documento ya venció.
4	1	Documento 1 - Firmado.pdf (creado y firmado manualmente para las pruebas)	Se utilizó la misma configuración de la prueba 1. Siguiendo las restricciones de firma del SNCD.	*<Indication> TOTAL_PASSED </Indication>*	El resultado incluye un mensaje informativo que indica que la CRL utilizada para validar el certificado de firma no es "fresca". La CRL se obtiene directamente del SNCD y al momento de ejecutar las pruebas la fecha de próxima actualización ya había pasado. *< Infos >The revocation freshness check is not concluant!</ Infos >*

Id	Esce-nario	Entradas		Salidas	
		Documento	**Política de validación de firma**	**Resultado**	**Observaciones**
5	1	Documento 2 - Firmado.pdf (creado y firmado manualmente para las pruebas)	Se utilizó la misma configuración de la prueba 1. Siguiendo las restricciones de firma del SNCD.	*<Indication> TOTAL_PASSED </Indication>*	Se generó el mismo mensaje de la prueba 4, que indica que la CRL utilizada para validar el certificado de firma no es "fresca".
6	2	Documento 3 - Modificado despues de firma.pdf (creado, firmado y modificado manualmente para las pruebas)	Se utilizó la misma configuración de la prueba 1. Siguiendo las restricciones de firma del SNCD.	*<Indication> TOTAL_PASSED </Indication>*	La aplicación identificó que la firma es válida, ya que los bytes del documento que se firmaron están intactos. Sin embargo, el documento es considerado inválido y se presentó la siguiente advertencia indicando que la firma cubre solamente cierta parte del documento: *<SignatureScope name="**Partial PDF**" scope="PdfByteRangeSignatureScope"> The document byte range: [0, 513690, 563228, 2295] </SignatureScope>*
7	2	CPSistemaNacionalCertificaciónDigitalversión1.pdf	Se modificó la política de validación. Se cambiaron los usos válidos del certificado de firma, para simular que el	*<Indication> TOTAL_FAILED </Indication>*	La aplicación identificó correctamente que el uso de certificado de firma no es válido, ya que el certificado incluido en la firma es para firma y no repudio.

Id	Esce-nario	Entradas		Salidas	
		Documento	**Política de validación de firma**	**Resultado**	**Observaciones**
		(tomado de la documentación del SNCD)	permitido es el de estampa de tiempo. *SignigCertificate – KeyUsage:* ~~***nonRepudiation***~~***,*** ~~***signature***~~ ***timestamp***		Junto con el resultado se indicó el siguiente error: *<Errors NameId="BBB_XCV_ISCGKU_ANS">* *The signer's certificate has not expected key-usage!* *</Errors>*
8	2	DCFD-Política-de-certificados-v1.1.pdf (tomado de la documentación del SNCD)	Se modificó la política de validación. Se cambiaron los algoritmos de hash y firma válidos para simular que el los válidos son los siguientes: *AcceptableEncryptionAlgo:* ~~***RSA***~~ ***ECDSA*** *AcceptableDigestAlgo:* ~~***SHA1, SHA256***~~ ***RIPEMD160***	*<Indication>* *TOTAL_FAILED* *</Indication>*	Se indicó que el algoritmo utilizado no está autorizado: *<Errors NameId="ASCCM_ANS_1">* *The encryption algorithm not authorized!* *</Errors>*

Id	Esce-nario	Entradas		Salidas	
		Documento	**Política de validación de firma**	**Resultado**	**Observaciones**
9	2	DCFD-Política-de-Formato-Oficial-v1.0.pdf (tomado de la documentación del SNCD)	Se utilizó la misma configuración de la prueba 1. Siguiendo las restricciones de firma del SNCD. Pero no se incluyó el certificado de la CA SINPE - Persona física, entre los certificados de confianza.	*<Indication> TOTAL_PASSED </Indication>*	La aplicación identificó que la firma es válida ya que no se presentaron problemas criptográficos. Sin embargo, el documento no es válido y se presentó la siguiente advertencia: *<Warnings>The certificate chain for timestamp is not trusted</Warnings>*
10	2	Documento 1 - Firmado.pdf (creado y firmado manualmente para las pruebas)	Se modificó la política de validación. Se cambió el formato válido para simular que el formato permitido es: *AcceptableFormats:* ***~~CAdES_BASELINE_T~~ XAdES***	*<Indication> TOTAL_FAILED </Indication>*	La firma se identificó como inválida, ya que contiene un formato no permitido por la política. Se generó el siguiente error: *<Errors NameId="BBB_FC_IEFF_ANS">The expected format is not found! </Errors>*
11	3	Documento formato desconocido 1 - Firmado.pdf (firmado con PKCS#7)	Se utilizó la misma configuración de la prueba 1. Siguiendo las restricciones de firma del SNCD.	*<Indication> TOTAL_FAILED </Indication>*	La firma se identificó como inválida, ya que contiene un formato no permitido en la política. Se generó el siguiente error: *<Errors NameId="BBB_FC_IEFF_ANS">The expected format is not found!</Errors>*

9.6. Apéndice F. Resultados de la evaluación de las políticas de seguridad para aplicaciones de verificación de firma digital y sello electrónico en la aplicación desarrollada

En este apéndice se presentan los resultados de la evaluación de las políticas de seguridad para aplicaciones de "verificación de firma digital y sello electrónico" en la aplicación desarrollada. En la **Tabla 19** se muestran las políticas y el resultado de evaluar si cada una de ellas se cumple o no en la aplicación desarrollada "Validador de formato de firma PAdES LTV". En la **Tabla 20** se presentan las observaciones de los resultados de la evaluación.

Tabla 19. Evaluación de las políticas de seguridad para aplicaciones de verificación de firma digital y sello electrónico en la aplicación desarrollada.

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
30	I	Se debe validar que el formato del documento electrónico cuyas firmas se van a verificar, está soportado por el SNCD y por la aplicación, y que además es correcto.	1	X			1
31	I	Se debe validar que el documento electrónico cuyas firmas se van a verificar, no contiene código oculto (por ejemplo, macros) o malicioso.	1	X			1

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
32	I	Se debe proteger el documento electrónico cuyas firmas se van a verificar, así como sus representaciones derivadas (resúmenes cifrados extraídos, documento electrónico original, resumen del documento electrónico original, resúmenes descifrados), mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	3			X	2
33	I	Se debe proteger el resultado de la validación del documento electrónico cuyas firmas se van a verificar, mientras se transmite por una red, de manera que no pueda ser modificada por usuarios no autorizados.	3			X	3
34	I	Se debe proteger los certificados digitales extraídos del documento electrónico cuyas firmas se van a verificar, mientras se transmiten por una red, de manera que no puedan ser modificados por usuarios no autorizados.	3			X	2
35	I	Se debe proteger el resultado de las validaciones de los certificados extraídos del documento electrónico cuyas firmas se van a verificar, mientras se transmiten por una red, de manera que no puedan ser modificadas por usuarios no autorizados.	3	X			4
36	I	Se debe proteger el resultado de las verificaciones de las firmas digitales, mientras se transmiten por una red, de manera que no puedan ser modificadas por usuarios no autorizados.	3	X			4

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
37	I	Se debe proteger el documento electrónico cuyas firmas se van a verificar, mientras transita por la memoria local, de manera que no pueda ser modificado por usuarios no autorizados.	4			X	5
38	I	Se debe proteger el resultado de la validación del documento electrónico cuyas firmas se van a verificar, mientras transita por la memoria local, de manera que no pueda ser modificada por usuarios no autorizados.	4			X	5
39	I	Se debe proteger el resultado de las validaciones de los certificados extraídos del documento electrónico cuyas firmas se van a verificar, mientras transita por la memoria local, de manera que no puedan ser modificadas por usuarios no autorizados.	4			X	5
40	I	Se debe proteger el resultado de las verificaciones de las firmas digitales, mientras transita por la memoria local, de manera que no puedan ser modificadas por usuarios no autorizados.	4			X	5
41	I	El *software* complementario requerido para ejecutar la aplicación, que incluye, pero no se limita al sistema operativo, navegadores de Internet, *frameworks*, *plug-ins* y *drivers*, debe tener instaladas las actualizaciones de seguridad más recientes.	5	X			6
42	A	Se debe validar que todos los certificados digitales contenidos en el documento electrónico cuyas firmas se van a verificar, pertenecen a la jerarquía nacional de certificadores registrados.	8	X			7

No.	Servicio de seguridad	Política de Seguridad	Objetivos de Control	Cumplimiento			Observa-ciones
				Sí	No	NA	
43	A	Se debe validar el uso correcto de los certificados digitales contenidos en el documento electrónico cuyas firmas se van a verificar.	11	X			8
44	C	Se debe proteger el documento electrónico cuyas firmas se van a verificar, así como sus representaciones derivadas (resúmenes cifrados extraídos, documento electrónico original, resumen del documento electrónico original, resúmenes descifrados), mientras se transmiten por red, de manera que no puedan ser revelados a usuarios no autorizados.	17			X	2
45	C	Se debe proteger el documento electrónico cuyas firmas se van a verificar, mientras transita por la memoria local, de manera que no pueda ser revelado a usuarios no autorizados.	20			X	5
46	C	Se debe validar que el acceso a recursos del sistema en el que se ejecuta la aplicación esté dado únicamente a usuarios o procesos autorizados.	18			X	5
47	C	Se debe prevenir el despliegue de datos que revelen detalles acerca de la configuración e implementación del sistema.	19	X			9
48	NR	Se debe validar que todos los certificados digitales, así como sus rutas de certificación, estaban vigentes cuando se incluyeron en el documento electrónico cuyas firmas se van a verificar.	22	X			10
49	NR	El resumen del documento electrónico cuyas firmas se van a verificar debe calcularse utilizando algoritmos *hash* seguros.	21	X			11

Tabla 20. Lista de observaciones de los resultados de evaluación.

No.	Observaciones
1	La aplicación incluye un mecanismo de control para verificar la entrada de información, en este caso un archivo. Tal y como se especifica en el objetivo de control verifica lo siguiente: • El archivo debe tener un formato permitido. • El formato del archivo debe ser correcto. • El tamaño del archivo no debe exceder un tamaño máximo permitido. Y como se explica en la **Sección 5.3 Diagrama de flujo de información de la aplicación** del **Capítulo 5**, previo al proceso de validación de un documento, este debe de ser analizado por un antivirus para verificar que no incluya contenido malicioso, como virus, *malware*, entre otros. Este mecanismo está contemplado a pesar de que no se implemente directamente en la aplicación.
2	La política no aplica en el contexto de la aplicación, ya que el tipo de dato que se menciona en la política no se envía a través de la red. La aplicación maneja esta información localmente en la memoria de la maquina durante la validación del documento. Una vez finalizado el proceso es eliminada.
3	La política no aplica en el contexto de la aplicación, el resultado de la validación del documento no se envía a través de la red. El resultado es almacenado localmente en una ubicación específica del disco duro de la máquina y solamente tienen acceso los usuarios que tengan permiso para acceder dicha ubicación. Este es un control de seguridad que queda fuera del contexto de la aplicación y depende de la infraestructura en donde se ejecute.
4	Este tipo de resultado de verificación si viaja en la red ya que se realizan consultas a servidores externos (CRLs, OCSP entre otros) y la aplicación permite utilizar un canal seguro para proteger la información. Es importante mencionar que, aunque la aplicación soporta un canal seguro, durante el proyecto no fue posible establecer la conexión por medio de https para obtener esta información, porque los *urls* incluidos en los certificados utilizados en el SNCD tienen las direcciones web con http.
5	La política no aplica en el contexto de la aplicación, el control de acceso no autorizado a la aplicación, a los datos y a los recursos del sistema debe implementarse a nivel de infraestructura.

No.	Observaciones
6	Para las librerías de terceros se utiliza la última versión disponible. Los otros controles relacionados con el antivirus y las actualizaciones de la máquina quedan fuera del contexto de la aplicación.
7	La aplicación implementa la validación de la cadena de certificados de los certificados de firma incluidos en el documento.
8	Para los certificados digitales incluidos en el documento, la aplicación valida el uso correcto de cada uno de ellos según la legislación de Costa Rica. Por ejemplo, para un certificado utilizado para firmar el documento se verifica que su uso sea para firma digital de documentos: *Digital Signature* y *Non-Repudiation*
9	La aplicación implementa un control de errores para no desplegar detalles sobre cualquier error que ocurra y que podría comprometer la seguridad del sistema.
10	La validación del estado de los certificados utilizados para firmar el documento forma parte del estándar europeo, por lo que la aplicación implementa este tipo de validaciones por medio de CRLs y OCSP.
11	La aplicación soporta algoritmos hash SHA-2 y superior. Sin embargo, también soporta otros algoritmos menos seguros por un tema de retrocompatibilidad. Si un documento fue firmado son SHA-1 mientras se consideraba un algoritmo seguro, la aplicación debe permitir validarlo, indiferentemente del resultado de validación. Esto depende del grado de tolerancia al riesgo del SNCD. Los algoritmos aceptados se configuran por medio de la política de validación de la aplicación.

9.7. Apéndice G. Objetivos de control para las políticas de verificación de firma digital y/o sello electrónico

En este apéndice se presentan los objetivos de control de la "*Guía de requerimientos técnicos para el aseguramiento de la información de los componentes tecnológicos que utilizan certificados y firma digital en aplicaciones de software dentro del Sistema Nacional de Certificación Digital*" [18] relacionados con las políticas de seguridad del escenario de uso "verificación de firma digital y/o sello electrónico". En la **Tabla 21** se muestra la lista de objetivos con sus identificadores y los de las políticas a las que aplican.

Tabla 21. Lista de objetivos de control que permiten evaluar el cumplimiento de las políticas.

No.	Servicio de seguridad	Objetivo de Control	Políticas
1	I	Se deben validar los datos que el usuario introduce en el sistema, verificando que cada entrada cumple al menos con los siguientes requisitos: *Cuando la entrada es texto* • Los caracteres introducidos deben ser válidos, según el conjunto de caracteres permitido correspondiente. • La longitud de los caracteres introducidos debe estar dentro de los límites mínimo y máximo correspondientes. • Si la entrada requiere un formato específico (como una fecha, una dirección de correo electrónico, un número telefónico, etcétera), los caracteres introducidos deben cumplir con ese formato. • Si la entrada se utiliza como argumento en una operación de creación, lectura, actualización o borrado de registros en una base de datos, se debe hacer a través de	30, 31

No.	Servicio de seguridad	Objetivo de Control	Políticas
		sentencias parametrizadas (*prepared statements*), y no mediante la concatenación de hileras de caracteres. • Si la entrada debe mostrarse al usuario posteriormente, durante su interacción con el sistema, deben aplicarse las reglas de escape correspondientes según el o los lenguajes utilizados. *Cuando la entrada es un archivo* • El archivo debe tener un formato permitido. • El formato del archivo debe ser correcto. • El tamaño del archivo no debe exceder un tamaño máximo permitido. • El archivo no debe almacenar contenido malicioso, como virus, *malware*, etcétera. Si el archivo se almacenará en el sistema de archivos de un servidor, su nombre o ubicación no debe ser igual al de algún archivo de configuración según el tipo de servidor. Por ejemplo, *.htaccess* en Apache, o *Web.conf* en IIS, entre otros.	
3	I	Los datos se deben transmitir por red utilizando algún protocolo que proporcione cifrado de datos, con una efectividad igual o superior a la ofrecida por TLS 1.0.	32, 33, 34, 35, 36
4	I	Se debe validar que las máquinas en las cuales se ejecutan componentes de la aplicación están libres de virus, *malware* y cualquier otro tipo de *software* malicioso que facilite la modificación no autorizada de datos, utilizando los siguientes criterios: *Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final* Se debe validar la existencia de un procedimiento periódico, ejecutado como máximo cada 7 días naturales, para comprobar que las máquinas no están infectadas. Se debe registrar una	37, 38, 39, 40

No.	Servicio de seguridad	Objetivo de Control	Políticas
		bitácora por máquina cada vez que el procedimiento se ejecuta, en la que se almacene al menos la siguiente información: • Nombre del responsable de ejecutar el procedimiento. • Fecha y hora en la que se ejecuta el procedimiento. • Identificador de la máquina. • Herramienta utilizada para ejecutar el procedimiento. • Lista de archivos analizados. • Resultado del análisis. *Cuando algún componente de la aplicación se ejecuta en una máquina que está bajo control total o parcial del usuario final* Se debe validar la existencia de documentación, entregada por el proveedor del software al usuario final, en la que al menos se indique: • Recomendaciones para mantener la máquina libre de infecciones. La importancia que tiene el mantener una máquina libre de infecciones, en lo que respecta al no repudio de la información.	
5	I	Se debe validar que el *software* complementario, requerido para ejecutar la aplicación, se encuentra actualizado en la máquina donde se ejecuta, utilizando los siguientes criterios: *Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final* Se debe validar la existencia un procedimiento periódico, ejecutado como máximo cada 7 días naturales, para comprobar que al menos el sistema operativo, los navegadores de Internet, los *frameworks*, los *plug-ins* y los *drivers* necesarios, están actualizados. Se debe	41

No.	Servicio de seguridad	Objetivo de Control	Políticas
		registrar una bitácora cada vez que el procedimiento se ejecuta, en la que se almacene al menos la siguiente información: • Nombre del responsable de ejecutar el procedimiento. • Fecha y hora en la que se ejecuta el procedimiento. • Identificador de la máquina. • Nombre del software comprobado. • Versión original del software. • Versión actualizada del software (si aplica). *Cuando algún componente de la aplicación se ejecuta en una máquina que está bajo control total o parcial del usuario final* Se debe validar la existencia de documentación, entregada por el proveedor del software al usuario final, en la que al menos se indique: • Recomendaciones para mantener el *software* complementario actualizado en la máquina. La importancia que tiene el mantener dicho *software* actualizado, en lo que respecta al no repudio de la información.	
8	A	La pertenencia del certificado digital a la jerarquía nacional de certificadores registrados se debe implementar mediante una validación que sea funcionalmente equivalente al algoritmo descrito en la sección 6.1 del RFC 5280	42
11	A	Se debe validar que el uso del certificado digital cumple con los requisitos establecidos en la sección 1.4.1 de la *Política de certificados para la jerarquía nacional de certificadores registrados* [5].	43

No.	Servicio de seguridad	Objetivo de Control	Políticas
17	C	Los datos se deben transmitir por red utilizando algún protocolo que proporcione cifrado de datos, con una efectividad igual o superior a la ofrecida por TLS 1.0.	44
18	C	Debe existir un contexto de encapsulamiento, en el que se definen al menos tres controles de autorización, los cuales deben satisfacerse antes de acceder a recursos del sistema.	46
19	C	La prevención del despliegue de datos que revelan detalles acerca de la configuración e implementación del sistema debe cumplir al menos con los siguientes requisitos: • Ningún tipo de información sensible debe mostrarse a través de mensajes de error, incluyendo, pero no limitándose a: detalles del sistema, identificadores e información de cuentas. • Se debe usar manejadores de errores que no despliegan información de depuración, ni *stack traces*. • Se deben implementar mensajes de error genéricos, y usar pantallas de error personalizadas. • Cuando corresponda, la aplicación debe manejar los errores que ocurren dentro de esta, y no delegar esa función en la configuración del servidor. La lógica de manejo de errores asociada a controles de seguridad debe denegar el acceso por defecto.	47
20		Se debe validar que las máquinas en las cuales se ejecutan componentes de la aplicación están libres de virus, *malware* y cualquier otro tipo de *software* malicioso que facilite la divulgación no autorizada de datos, utilizando los siguientes criterios: *Cuando algún componente de la aplicación se ejecuta en una máquina que no está bajo control total ni parcial del usuario final*	45

No.	Servicio de seguridad	Objetivo de Control	Políticas
		Se debe validar la existencia de un procedimiento periódico, ejecutado como máximo cada 7 días naturales, para comprobar que las máquinas no están infectadas. Se debe registrar una bitácora por máquina cada vez que el procedimiento se ejecuta, en la que se almacene al menos la siguiente información: • Nombre del responsable de ejecutar el procedimiento. • Fecha y hora en la que se ejecuta el procedimiento. • Identificador de la máquina. • Herramienta utilizada para ejecutar el procedimiento. • Lista de archivos analizados. • Resultado del análisis. *Cuando algún componente de la aplicación se ejecuta en una máquina que está bajo control total o parcial del usuario final* Se debe validar la existencia de documentación, entregada por el proveedor del software al usuario final, en la que al menos se indique: • Recomendaciones para mantener la máquina libre de infecciones. La importancia que tiene el mantener una máquina libre de infecciones, en lo que respecta al no repudio de la información.	
21	NR	Se debe validar que los algoritmos de *hash* utilizados son seguros, y tienen una efectividad igual o superior a SHA-2, y rechazar los demás.	49
22	NR	La validación de la vigencia del certificado debe cumplir con los siguientes requisitos: • Se debe verificar que el certificado se encuentra activo, es decir, que no ha expirado ni ha sido revocado o suspendido.	48

No.	Servicio de seguridad	Objetivo de Control	Políticas
		• Se debe evaluar la vigencia del certificado, y la vigencia de todos los certificados de las CA en la ruta de certificación a la que pertenece el certificado. La información de revocación se debe obtener a partir de CRLs u OCSP, de acuerdo con el grado de tolerancia al riesgo.	